UNIVERSITÀ
DI SIENA
1240

DIPARTIMENTO DI GIURISPRUDENZA

Dottorato di ricerca in "Scienza Giuridiche"

XXXIII Ciclo

Il captatore informatico.

Strumento investigativo "obsoleto" ma ancora privo di una stabile disciplina normativa

Tutor

Chiar.mo Prof. Sergio Lorusso

di dottorato di
nda Nocerino

A mamma, papà, Raffaele e L.,
al loro immenso amore

IL CAPTATORE INFORMATICO

STRUMENTO INVESTIGATIVO "OBSOLETO" MA ANCORA PRIVO DI UNA STABILE DISCIPLINA NORMATIVA

INDICE

CAPITOLO II

IL LATO OSCURO DELLE RIFORME:

IL CAPTATORE INFORMATICO OLTRE I CONFINI DELLE INTERCETTAZIONI

CAPITOLO III

LE APORIE APPLICATIVE DELLA NORMATIVA

CAPITOLO IV
L'IMPATTO SUI DIRITTI FONDAMENTALI

CAPITOLO V
IL CAPTATORE INFORMATICO NELLE INDAGINI PROATTIVE

IL CAPTATORE INFORMATICO NEL PROCESSO PENALE. COS'È. CHI LO USA. CHI NON LO USA PIÙ.

La rivoluzione informatica degli ultimi tempi ha profondamente modificato le abitudini degli individui, alterandone il modo di vivere, comunicare, interagire e intendere i rapporti interpersonali. Relazioni affrancate dalla dimensione fisica e materiale che cede il posto a quella eterea; intersezioni di sguardi, gesti, parole sostituite da algide digitazioni su scatole meccaniche che sembrano rappresentare l'unica interfaccia dell'uomo moderno. Una realtà, questa, che inevitabilmente involge e travolge prepotentemente anche il mondo del diritto, determinando un effetto domino che si ripercuote sui più o meno tradizionali istituti giuridici, imponendone una furente modernizzazione nell'ottica della creazione di una «giustizia penale 2.0» (S. Lorusso, Digital evidence, cybercrime *e giustizia penale 2.0,* in *Proc. pen. giust.,* 2019, f. 4, p. 821 ss.).

Per quel che in questa sede rileva, non può sottacersi come allo sviluppo tecnologico dei rapporti sociali faccia da *pendant* il mutamento ontologico delle fattispecie di reato: per un verso, la criminalità, abbattendo i troppo angusti confini interni, assume i connotati della transnazionalità, dispiegando le sue potenzialità *ubicumque*; per l'altro, muta le sue caratteristiche tradizionali per manifestarsi interamente sulla rete (c.d. *cybercrime*) ovvero per il tramite della rete (c.d. *computer crime*).

Una metamorfosi socio-culturale così radicale incide sulle scelte di politica-criminale volte ad adeguare la risposta sanzionatoria all'effettiva esigenza o emergenza da contenere, perché «il compito del diritto è mettere in ordine la società; aiutare a dare a ciascuno ciò che non ha ma deve avere. Il compito del diritto e del processo penale è ancora più alto; la pena deve trasformare il *malum* in *bonum passionis*, insegnando all'uomo e alla società ad essere ciò che non è ma deve essere» (F. Carnelutti, *Teoria generale del reato*, Cedam, 1933, p. 7).

D'altra parte, se le informazioni relative ad un reato, informatico o comune, sono potenzialmente in grado di "transitare" dal mondo digitale, diviene di fondamentale importanza plasmare le tecniche investigative alle nuove fonti di prova digitale mediante una specifica preparazione tecnologica e l'apprestamento, per via legislativa, di un reticolo normativo capace di disciplinare la materia, «considerato che è inevitabile prevedere una sempre maggiore diffusione della *digital evidence* nel mondo giuridico» (L. Luparia, Computer crimes *e procedimento penale*, in AA. VV., *Modelli differenziati di accertamento*, a cura di G. Garuti, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, 2011, p. 374).

Di conseguenza, su un versante più propriamente processuale, si registra un frenetico ricorso a nuovi strumenti di indagine ad alto contenuto tecnologico che risultano indispensabili a rendere effettiva la lotta contro le più evolute forme di criminalità. Progredendo, infatti, con straordinaria velocità tanto le tecnologie di captazione - che diventano sofisticate ed invasive - quanto le tecniche di elusione di ogni captazione

possibile - che si affidano all'impenetrabilità degli apparecchi utilizzati, all'inaccessibilità di particolari reti di captazione ovvero all'adozione di sistemi di criptazione dei messaggi scambiati -, risulta imprescindibile affidarsi ad avanzati strumenti tecnologici per scardinare i canali criminali di comunicazione o scambio di informazioni utilizzati per la commissione di reati di particolare allarme sociale.

Proprio in questo contesto, i captatori informatici rivestono un ruolo centrale nelle investigazioni di polizia, dal momento che, abbattendo i tradizionali sistemi di cifratura e le eventuali tecniche di *anti forensics,* offrono la possibilità di un pieno controllo del sistema su cui vengono inoculati.

In particolare, il captatore informatico è un *software* (o, più correttamente, un *malware*) che, in maniera nascosta, s'infiltra (manualmente in modalità *off-line,* o attraverso internet, con attività di *social engeneering* o agendo sulle *defaillances* dell'apparecchio elettronico) in apparati informatici come *smartphone,* computer e *tablet,* e – con comandi attivati da remoto– compie molteplici attività, esportando i relativi risultati informativi verso il *server* cui è collegato. Può intercettare flussi di comunicazioni tra sistemi informatici e telematici (posta elettronica, messaggistica come *whatsapp,* conversazioni *Voip* come *Skype,* attività di *screenshot* e di *keylogging*), attivare microfono e/o telecamera e rilevatori GPS, eseguire attività di *Trojan*, vale a dire entrare nella memoria dei dispositivi in cui sono conservati i dati e, conseguentemente, acquisire tutti i dati e le informazioni *ivi* contenute o transitanti sul dispositivo infettato.

Sin dall'inizio del percorso evolutivo che ha condotto ad una regolamentazione del "nuovo" strumento investigativo nel 2017 (D.lgs. 29 dicembre 2017, n. 216, recante "*Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a, b, c, d ed e, della legge 23 giugno 2017,* n. 103", in *Gazz. uff.,* 11 gennaio 2018, n. 8), è emersa la straordinaria polivalenza del *virus* informatico, capace di realizzare, attraverso un meccanismo tecnologico di semplice implementazione, gli effetti di una pluralità di mezzi di ricerca della prova, sia tipici che atipici: le intercettazioni telefoniche, ambientali, di comunicazioni informatiche o telematiche, la perquisizione di un sistema informatico o telematico, il sequestro di dati informatici, le videoriprese, il pedinamento elettronico. Il tutto, per giunta, nei confronti di una cerchia di soggetti potenzialmente indeterminata, costituta da tutti coloro che ricadono nel raggio di azione del dispositivo "infetto".

Proprio in ragione della sua intrinseca poliedricità, il captatore informatico per lungo tempo è stato impiegato nel procedimento penale per scopi assai diversi: talvolta, come strumento investigativo inedito per condurre atti "tipici" di indagine ossia espletare tradizionali mezzi di ricerca della prova (Sez. un., 28 aprile 2016, n. 26889, in *Cass. pen.,* 2016, p. 3546 ss.); talaltra, per condurre atti di indagine del tutto "nuovi" e di difficile inquadramento giuridico, sperimentando nuove categorie di mezzi di ricerca della prova atipici (Sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.,* n. 246954); altre volte ancora per condurre contemporaneamente tutte le attività investigative tipiche e atipiche contemporaneamente (Sez. VI, 26 maggio 2015, n. 27100, in *C.E.D. Cass.,* n. 265655).

La peculiarità dello strumento in esame, tuttavia, non rileva esclusivamente nella sua polivalenza funzionale, risultando caratterizzato da un esasperato protagonismo che lo rende indispensabile non solo nella fase procedimentale delle indagini preliminare ma anche durante l'espletamento delle investigazioni preventive. Più precisamente, il

malware non trova impiego esclusivo nelle indagini di polizia *strictu sensu* intese, risultando ampiamente utilizzato anche nella fase volta all'esplorazione dei dati funzionali alla ricerca della *notitia criminis*: a fronte di un sostanziale mutamento del sistema penale che arretra i suoi argini ad una fase pre-procedimentale, il captatore informatico diventa lo strumento privilegiato con il quale gli operatori danno luogo ad intercettazioni e controlli preventivi sulle comunicazioni (art. 226 disp. att. c.p.p.) che, come noto rappresentano tipici strumenti, non propriamente di indagine ma di investigazione, impiegati dalle Forze di polizia e dagli organi di *intelligence* governativa per evitare la commissione di gravi reati di criminalità organizzata e terrorismo.

Ma non solo. Al di là di questa *species* di indagine preventiva, nella prassi investigativa esistono altre forme di sorveglianza "anticipata" che, pur non trovando espressa regolamentazione, risultano assai utili nella prevenzione del crimine, in quanto indirizzate all'acquisizione di informazioni necessarie a far emergere sospetti che legittimano il compimento delle attività preventive tipizzate ovvero elementi funzionali alla formazione della notizia di reato. Simili attività monitoranti vengono eseguite mediante l'ausilio di strumenti *iper* tecnologici che, facilitando la raccolta massiva di dati e di informazioni, configurano quali strumenti privilegiati per espletare attività di sorveglianza non mirata, funzionale al controllo *ex ante* di gruppi di soggetti non identificati ma individuati sulla scorta dei criteri elaborati attraverso l'uso proattivo dei dati, funzionali, almeno in tesi, a svelare sospetti criminali o terroristi ancora ignoti.

A fronte di una simile poliedricità funzionale e occupazionale, nessun dubbio può sorgere sulla speciale utilità – per non dire "indispensabilità" – di un simile strumento in una fase storica che ha conosciuto una rapidissima evoluzione sia del sistema globale delle comunicazioni sia delle modalità di azione degli ambienti criminali. Di qui, «[R]rinunciare al captatore informatico significherebbe portare la giustizia penale al di fuori dell'era contemporanea» (A. Balsamo, *Il magistrato*, in AA. VV., *Nuove norme in tema di intercettazioni*, a cura di G. Giostra-R. Orlandi, Giappichelli, 2012018, p. 336 s.).

Altrettanto evidente è, però, la particolare dimensione del pericolo per i diritti e le libertà insito nella straordinaria invasività delle nuove tecniche acquisitive che possono determinare un controllo totale e totalizzante della vita di un numero assai elevato di individui, anche solo indirettamente coinvolti nel circuito processuale o, addirittura, completamente estranei allo stesso. E così l'essere umano, portatore di valori, prerogative e garanzie, si trasformerebbe nell'hitleriano "uomo di vetro", «sospetto e cattivo cittadino [perché] intende mantenere spazi di intimità o di esercizio libero di diritti» (S. Rodotá, *Prefazione a D. Lyon, La società sorvegliata. Tecnologie di controllo della vita quotidiana,* Feltrinelli, 2003, p. XIV).

La rilevanza della *quaestio de qua* nel panorama interno ed internazionale appare, quindi, indiscutibile. Ciò non solo alla luce della recente attuazione della tortuosa regolamentazione normativa che potrebbe operare una "rivoluzione copernicana" delle indagini con evidenti ricadute sia nell'ambito processuale che *extra*-processuale, ma anche in ottica "futuristica": l'irrefrenabile velocità con cui gli strumenti investigativi si evolvono apre la strada all'impiego di ulteriori tecniche di indagini (intelligenza artificiale, droni, *robot*) che, spingendosi assai oltre i confini legislativi previsti in relazione all'uso del captatore informatico, sono destinati a comprimere – inevitabilmente

– fondamentali diritti degli individui, nel frattempo privati di adeguate forme di tutela nell'assenza di una normativa che li contempli.

In questo quadro magmatico e perturbante, l'intervento del giurista appare tanto necessario quanto doveroso.

Di fronte ad un così tangibile cambiamento culturale, lo studioso non può rimanere confinato nel suo *habitat* naturale senza avere contezza del mutamento che lo circonda; al giurista è chiesto di scendere nell'arena dove il diritto processuale penale deve fare i conti con i difficili problemi dell'attuale società. Dismessi i panni di puro "umanista", lo studioso del diritto finisce per assumere le vesti di un "giurista tecnologico" che è capace di adeguare il diritto alla realtà contingente: come, infatti, sostenuto, «al progresso inevitabilmente deve adeguarsi il processo, pena la trasformazione [dello stesso] in un'arma spuntata, inidonea a raggiungere lo scopo» (C. Conti, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* in *Dir. pen. proc.,* 2018, p. 1210) .

Tuttavia, il cambiamento atteso non è di facile concretizzazione.

Quello delle *scientiae* forensi è un terreno assai impervio che risulta quanto mai scivoloso per il giurista; una zona grigia, oscura e, al contempo, pericolosa per i "tradizionalisti", non solo perché impone una metamorfosi, una rinnovazione, un cambiamento ma anche nell'ottica di un possibile depauperamento del sostrato culturale che governa il sistema.

Nulla di nuovo, potrebbe obiettarsi. L'irrompere nell'accertamento penale delle nuove metodologie investigative impegna l'interprete in un dibattito simile a quello che qualche anno fa vide impegnata dottrina e giurisprudenza in ordine al prepotente ingresso della prova scientifica con il conseguente problema di arginare la *junk science* ed il materiale probatorio inquinato.

Eppure, in questa naturale tensione verso l'etere digitale si profila il rischio della potenziale deriva tecnicista del giurista che può cedere all'eccesso e approcciarsi al sistema senza tener conto dei principi che lo governano, anelando ad una rinnovazione del processo penale al fine della rigorosa ricerca del vero e della verità, finendo per rinnegare gli stessi valori che lo hanno ispirato. Di fronte ad un tecnicismo così esasperato e condizionante l'accertamento, il processo penale, per evitare di perdere la propria identità deve aggrapparsi ai diritti fondamentali, in assenza dei quali il rischio di un «processo come laboratorio scientifico, affidato ad asettici operatori in camice bianco» (E. Amodio, *La rinascita del diritto delle prove penali. Dalla teoria romantica delle* intime conviction *al recupero della legalità probatoria*, in AA. VV., *Processo penale, diritto europeo e* common law*: dal rito inquisitorio al giusto processo*, a cura di E. Amodio, Giuffrè, 2003, p. 128), rischia di divenire realtà.

La difficoltà in cui il "moderno" giurista si trova, dunque, è la frenetica ricerca dell'equo bilanciamento tra accertamento del fatto - facilitato dal frequente utilizzo di nuovi strumenti di indagine ad alto potenziale tecnologico - e tutela dei diritti fondamentali di ogni individuo; ricerca che non può spingersi fino a determinare un'eterogenesi dei fini, laddove le derive antiformalistiche, avallate sempre più spesso dal legislatore e dalla giurisprudenza costituzionale e sovranazionale, allontanano il sistema dall'ineludibile principio di legalità processuale che presidia la tutela dei valori fondanti l'ordine costituito (G. Ubertis, *Equità e proporzionalità* versus *legalità processuale: eterogenesi dei fini?,* in *Arch. pen*., 2017, p. 389 ss.) .

In ragione di queste premesse, sia consentito un ringraziamento a quanti hanno permesso di attraversare gli imperscrutabili canali delle investigazioni tecniche con uno spirito di collaborazione e di progressivo avvicinamento tra l'"etereo" mondo del diritto e chi, per contro, sulla base di quelle norme, deve agire ogni giorno, nella consapevolezza che solo un rapporto simbiotico tra teoria e prassi conduce al raggiungimento di un obiettivo comune: la ricerca di "una" verità, giusta sintesi tra quella storica e quella processuale.

CAPITOLO I

IL CAPTATORE INFORMATICO TRA PRASSI E DIRITTO

SOMMARIO: 1. Gli aspetti tecnico-operativi del *Trojan Horse* – 1.1. *Segue*: funzionalità e potenzialità investigative – 2. Il *virus* di Stato nella giurisprudenza di legittimità: da arnese per le investigazioni "*ad explorandum*" a strumento di intercettazione "ambientale" – 2.1. *Segue*: la risoluzione del conflitto ad opera delle Sezioni Unite – 3. Da *querelle* giurisprudenziale a priorità parlamentare. Le proposte di legge per una dignità normativa ai nuovi strumenti investigativi – 4. Il captatore informatico nella *maxi* riforma "Orlando". Criteri direttivi – 5. Il d.lgs. 216/2017. Esegesi di una disciplina "fantasma" – 5.1. *Segue*: i divieti di utilizzazione del captato – 5.2. *Segue*: il "terzo binario" investigativo per i reati contro la pubblica amministrazione – 6. Il progressivo ampliamento delle fattispecie intercettabili. La legge "Spazzacorrotti" – 7. La "riforma della riforma fantasma": dal d.l. 161/2019 alla l. 7/2020.

1. GLI ASPETTI TECNICO-OPERATIVI DEL *TROJAN HORSE*

In tema di investigazioni tecnico-scientifiche, nessuna considerazione giuridica può prescindere dalla conoscenza tecnica degli strumenti attraverso i quali le indagini vengono condotte. Ciò perché i nuovi ritrovati della tecnica e delle scienze non offrono solo nuove modalità di esecuzione di "vecchi istituti processuali" ma, spesso, rappresentano attività inedite, "casi" e "modi" originali, che mal si conciliano con le categorie probatorie esistenti e richiedono un'attenta analisi dello studioso, degli operatori del diritto e della giurisprudenza, sulla loro compatibilità con le libertà costituzionali che tendono ad invadere.

Tra questi, un posto di centrale rilievo, vuoi per la attualità della disciplina normativa vuoi per minaccia ai presidi difensivi, riveste l'uso del captatore informatico nel processo penale[1].

[1] Per una disamina della *quaestio* relativa al prepotente ingresso del captatore informatico nel circuito processuale, v., sin d'ora, M.T. ABBAGNALE, *In tema di captatore informatico*, in *Arch. pen*., 2016, f. 2, p. 13 ss.; G. AMATO, *Per l'uso del* "trojan" *compromesso non facile sulle regole*, in *Guida dir.,* 2018, f. 7, p. 55 ss.; S. ATERNO, voce Digital forensic *(investigazioni informatich*e), in *Dig. disc. pen*., Agg. VIII, Utet, 2014, p. 217 s.; A. BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*, in *Cass. pen*., 2016, f. 5, p. 2274 ss.; P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in. *Riv. it. sc. giur*., 2017, f. 8, p. 329 ss.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de Direito Processual Penal,* Porto Alegre, 2017, vol. 3, f. 2, p. 483 ss.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen*. online, 2014, p. 1; M. DANIELE, *Contrasto al terrorismo e captatori informatici,* in *Riv. dir. proc*., 2017, f. 3, p. 393 s.; D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *Jusonline,* 2017, f. 3, p. 385; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust*., 2016, f. 5, p. 120 ss.; A. GAITO-S. FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen*., 2016, f. 2, p. 309 ss.; P. MAGGIO, *La registrazione occulta curata da una persona presente al colloquio*, in AA. VV., *Le indagini atipiche*, a cura di A. Scalfati, II ed., 2019, p. 88 ss.; R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, f. 2, p. 538 ss.; P. RIVELLO, *Le intercettazioni mediante captatore informatico*, in AA. VV., *Le nuove intercettazioni*, a cura di O. Mazza, Giappichelli, 2018, p. 101; A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite virus informatico*, in AA. VV., *Le indagini*

Strumento di indagine inedito per i giuristi ma già da tempo utilizzato dagli investigatori che si servono del *virus* per insinuarsi nei canali criminali di comunicazione e, sfruttando la sua duttile natura camaleontica, monitorare lo scambio di informazioni che transitano sui dispositivi elettronici interessati[2].

Già la sua denominazione crea frizioni tra gli interpreti del diritto[3]. C'è chi lo chiama *Trojan Horse*, per evocare «l'agguato del caval»[4] che permise ai greci di penetrare le invalicabili mura della città di Ilio[5]; chi lo definisce quale "*virus* informatico"[6] o "di Stato"[7], per sottolineare la sua invasività; chi lo appella come "programma spia", facendo leva sulla mole di informazioni acquisibili mediante il suo ausilio; chi, ancora, lo qualifica come "agente intrusore informatico", ricorrendo a «tre concetti semplici e diretti: l'agire, l'intrusione, l'àmbito informatico»[8].

Ma, ormai, le resistenze dei "puristi" devono ritenersi superate. Il legislatore, infatti, fornisce allo strumento in esame una precisa nomenclatura, definendolo "captatore

atipiche, II ed., cit., p. 601 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 237; A. TESTAGUZZA, voce Virus *informatico*, in *Dig. disc. pen*., X, Utet, 2018, p. 931 ss.; ID., *I sistemi di controllo remoto: fra normativa e prassi,* in *Dir. pen. proc*., 2014, f. 6, p. 759 ss.; P. TONINI, *I captatori informatici*, in *Jusonline,* 2017, f. 3, p. 383 ss.; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017, p. 10 ss.; ID., *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc*., 2015, f. 9, p. 1163 ss.

[2] «Qualche *byte* di codice, in un programma per computer, un *virus* si potrebbe dire […]. Un esempio di una tecnologia "da *hacker*" utilizzata per fini nobili: come un Robin Hood che intercetta gli indagati per aiutare la giustizia». Così A. SGERZA, *Un* virus *per pc inchioda Bisignani. Lo Stato diventa* hacker *a fin di bene,* in *www.repubblica.it*, 22 giugno 2011.

[3] Per una panoramica sulle differenti terminologie impiegate per riferirsi al captatore informatico, M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 12 s.

[4] D. ALIGHIERI, *Divina commedia. Inferno*, canto XXVI, v. 59.

[5] In dottrina si è evidenziato, con metafora epica, che «il *virus trojan* prende il suo nome, verosimilmente, dal leggendario cavallo di Troia che, per mezzo di Odisseo, l'uomo dal multiforme ingegno, riuscì ad entrare dentro le mura di Troia, con inganno, ed espugnarla. Così come il cavallo di Troia sconfisse i troiani entrando all'interno della loro cittadella muraria, fingendosi un dono pregiato da parte degli Achei, così anche il predetto virus riesce ad entrare, con inganno, nell'apparecchio […] che si vuole intercettare, non per distruggerlo né tanto meno per danneggiarlo, ma per carpire qualsiasi dato che *ivi* possa trovarvi». Così M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Dir. pen. cont*., 2018, f. 2, p. 23.

[6] Da un punto di vista tecnico, l'assimilazione del captatore informatico ai *virus* informatici appare alquanto impropria dal momento che, a differenza di questi ultimi, il *Trojan* non si propaga verso altri dispositivi. Sottolinea tale diversità R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, in AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra-R. Orlandi, Giappichelli, 2018, p. 219.

[7] Denominazione che poco convince l'interprete in ragione della completa gestione delle operazioni *de quibus* da parte di società private, italiane e straniere. Sul punto, si rinvia a Cap. III, § 7.

[8] Così D. MINOTTI, *Captatori informatici: per un ponte tra diritti e informatica*, in AA. VV., Trojan horse: *tecnologia, indagini e garanzie di libertà (profili di* intelligence) in *www.parolaalladifesa.it*, 6 settembre 2016, p. 168.

informatico"[9], probabilmente rappresentando solo parzialmente le sue infinite potenzialità[10].

A prescindere dalle disquisizioni sulle più pertinenti designazioni, può dirsi che nessun dubbio si ravvisa in ordina alla sua identità che, in prima approssimazione, presenta i caratteri della imperscrutabilità[11] e dell'incontrollabilità da parte del monitorato[12].

[9] Cfr. Legge 23 giugno 2017, n. 103, recante "*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*", in *Gazz. uff.* 4 luglio 2017, n. 154, prevede, nell'esercizio della delega di cui al comma 82, che vengano attuati decreti legislativi recanti una nuova forma di intercettazione di conversazioni o comunicazioni tra presenti attraverso l'immissione, in dispositivi elettronici portatili, del c.d. captatore informatico. L'espressione de qua è proposta, in sostituzione di quella di "*virus*", dal Presidente D'Ascola, nella seduta del 1 agosto 2016 in sede di II Commissione Permanente.

[10] Per una panoramica sui potenziali usi processuali del captatore informatico alla luce delle sue caratteristiche tecniche v. S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, in AA. VV., IISFA Memberbook, a cura di G. COSTABILE-A. ATTANASIO, Experta, 2013, p. 1 ss.; ID., *Il* trojan *dalla A alla Z. Esigenze investigative e limitazioni della* privacy: *un bilanciamento necessario*, in *www.dirittopenaleinformatica.it;* R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., p. 221 ss.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, in *Dir. pen. cont*., 2018, f. 11, p. 51 s.; L. CUOMO, *La prova digitale*, in AA. VV., *Prova scientifica e processo penale*, a cura di G. Canzio-L. Luparia, Wolters Kluwer-Cedam, 2018, p. 722 ss.; W. NOCERINO, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale,* in *Cass. pen.,* 2016, f. 10, p. 3567 ss.; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 101; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 237 ss.; A. TESTAGUZZA, voce Virus *informatico*, cit., p. 931 ss.; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 13 ss.; G. VACIAGO, Digital evidence. *I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato,* Giappichelli, 2012, p. 12 s.; G. ZICCARDI, *La procedura di analisi della fonte di prova digitale,* in AA. VV., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* a cura di L. Luparia-G. Ziccardi, Giuffrè, 2007, p. 44; M. ZONARO, *Il* Trojan – *Aspetti tecnici e operativi dell'utilizzo di un innovativo strumento di intercettazione*, in *Parola alla difesa,* 2016, f. 1, p. 166 ss.

[11] Si parla di imperscrutabilità dal momento che il *malware* opera in modalità *stealth*, ossia celata agli occhi del titolare della macchina bersaglio, in modo da non poter essere rilevata da alcun sistema di protezione del dispositivo infettato (*antivirus*).

[12] Come meglio si dirà tra breve, il captatore informatico compie attività che permettono un controllo indiscriminato ed incondizionato dell'apparecchio sui cui il *malware* viene installato. Come sostenuto, «il controllo dell'indagato è talmente pervasivo da non avere, almeno potenzialmente, più alcun limite di spazio e di tempo». Così S. LONATI, *I criteri direttivi contenuti nella delega in materia di intercettazioni*, in AA. VV., *Le nuove intercettazioni*, cit., p. 22.

Più nel dettaglio, si tratta di un *software* (*rectius malware*)[13] appartenente alla categoria dei "sistemi informatici di controllo remoto"[14] (*Remote Control System*)[15], dal momento che consente di manovrare a distanza la macchina bersaglio attraverso una connessione di rete da un qualsiasi altro calcolatore, sfruttando un'architettura di tipo *client/server*. Attraverso quest'ultimo, abbattendo la protezione del dispositivo, il captatore penetra nell'apparato oggetto di indagine; mentre tramite il *client* il monitorante ne acquisisce il controllo.

Tentando una semplificazione, può dirsi che i protagonisti della procedura di infiltrazione sono due (o più)[16] sistemi elettronici (*smartphones, computers*, fissi o portatili, *tablets*) dotati di una connessione internet, sia essa *wi-fi* sia essa *ethernet*[17]: un dispositivo *target* infettato dal *server* sempre in ascolto e in grado di ricevere ed eseguire istruzioni specifiche trasmesse dall'apparato controllante e un calcolatore dotato del modulo *client* con funzione di *controller* per far compiere alla macchina bersaglio qualsiasi operazione.

L'aggressione del dispositivo da attenzionare viene tecnicamente definita "inoculamento". Esso può avvenire a distanza, sfruttando come veicolo programmi ingannevoli, oppure mediante un contatto fisico diretto sulla macchina bersaglio[18].

Nel primo caso, il *malware* viene istallato con la collaborazione attiva inconsapevole del soggetto da monitorare, sfruttando tecniche di *social engineering*[19], ossia attaccando

---

[13] In ambito di sicurezza informatica, il termine *malware* indica genericamente un qualsiasi *software* creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o ad un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* ed ha dunque il significato letterale di "programma malvagio". *Malware*, in realtà, è concetto di genere che comprende tutte le diverse *species* di *virus* conosciuti: *virus* in senso stretto (*virus* di *file*, *virus* di *boot*, *virus* multipartiti e *virus* di *macro*), *worms*, *trojan* e *backdoors*. Da un punto di vista informatico, un *virus* non è altro che un programma che si attiva e comincia a diffondersi in modo totalmente indipendente dalla volontà dell'utente. I *virus* non sono capaci di un comportamento autonomo: tutto ciò che sono in grado di fare è stato puntualmente previsto (come un qualsiasi programma per computer) dai programmatori che li hanno ideati e scritti. Cfr. A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, Cedam, 2015, p. 80 ss.

[14] «[…] il "remote" dell'inglese può designare una attitudine a proiettarsi nel futuro mediante il superamento della distanza nello spazio, così da comandare azioni che si realizzano in luoghi diversi». Così E. AMODIO, *Smettiamo di storpiare l'italiano con il lugubre "da remoto"*, in *Sist. pen*., 28 aprile 2020, il quale, soffermandosi sulla natura ambigua del termine, sottolinea l'inopportunità del ricorso alla tecnica *de qua*.

[15] V., sul punto, A. TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi,* cit., p. 759 ss.

[16] Secondo parte della dottrina, le potenzialità tecniche del captatore informatico consento non solo il monitoraggio in tempo reale del dispositivo bersaglio, bensì anche di terzi apparecchi allo stesso collegati da una rete LAN. In altre parole, l'agente intrusore «può monitorare pure i dispositivi, anche appartenenti terzi, che siano collegati mediante una rete locale al dispositivo informatico su cui è stato installato il *trojan*». Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 239.

[17] A titolo esemplificativo si possono citare gli *smartphone*, *tablet*, PC, *laptot*, *Smart* TV, autovetture e, più in generale, qualsiasi dispositivo dotato di tecnologia *Smart*.

[18] Sul punto, R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., p. 219; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 51 s.; S. LONATI, *I criteri direttivi contenuti nella delega in materia di intercettazioni*, cit., p. 22 s.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 238 s.

[19] «Nel campo della sicurezza delle informazioni per ingegneria sociale (dall'inglese *social engineering)* si intende lo studio del comportamento individuale di un soggetto al fine di carpirne

l'identità elettronica mediante una particolare tecnica psicologica che sfrutta l'inesperienza e la buona fede degli utenti allo scopo di carpire informazioni personali in vista di un successivo accesso ai sistemi protetti.

Più precisamente, il collegamento tra il *client* e il *server* viene realizzato attraverso l'invio, tramite la rete Internet, di un programma tipo *Trojan,* costituito da una componente nota all'utente - il quale installa il programma proprio per ottenerne le funzionalità a lui familiari - e una componente sconosciuta, rappresentata da quella parte del programma che cela un codice segreto in grado di creare un collegamento occulto tra il dispositivo su cui è installato il *server* e il computer remoto di controllo.

Nella seconda ipotesi, invece, l'inoculazione avviene tramite un intervento tecnico materiale a livello *hardware* sul dispositivo da controllare. Anche in tal caso la buona riuscita del monitoraggio deriva dalla collaborazione (in questo caso "passiva") del soggetto da controllare il quale deve lasciare incustodito l'apparecchio per il tempo necessario per l'intervento fisico da parte dell'operatore di polizia giudiziaria o del suo ausiliario[20].

Dalla sommaria descrizione operata, emerge che la procedura di inoculamento non è di semplice realizzazione. Ciò per diverse ragioni.

In primis, si rilevano difficoltà di ordine tecnico. I captatori informatici, come ogni strumento tecnologico, sono soggetti a rapida obsolescenza e, di conseguenza, i più aggiornati *software antivirus* potrebbero impedirne l'ingresso e rivelarne la presenza. Inoltre, la trasmissione dei dati in uscita dal sistema bersaglio al *server* di ascolto potrebbe essere individuata da programmi *ad hoc*.

Per ridurre un simile rischio, rivelano gli esperti, i pacchetti dati dovranno essere opportunamente occultati in mezzo alla trasmissione di altri dati e gli indirizzi IP del ricevente mascherati attraverso il passaggio da ulteriori *server* (*proxy*), interposti tra *server* e *client*[21].

Alle difficoltà proprie della *digital forensics* si associano *impasse* di ordine pratico.

Intanto, non sempre è possibile fare affidamento sull'ignara collaborazione del controllato, soprattutto quando le investigazioni sono dirette al monitoraggio di soggetti inseriti in particolari contesti criminali, avvezzi a diffidare da *input* provenienti da fonti sconosciute e, molto spesso, assistiti da consulenti estremamente competenti in materia di sicurezza informatica. In questi casi, l'unica alternativa per ottenere il controllo da remoto del dispositivo *target* consiste nell'affidarsi alla collaborazione del gestore del

---

informazioni. Un ingegnere sociale (*social engineer*) per definirsi tale, deve saper fingere, essere in grado di ingannare gli altri, deve saper nascondere la propria identità e fingersi un'altra persona: in tal modo egli riesce a ricavare informazioni che non potrebbe mai ottenere con la sua reale identità. Sul punto K.D. MITNICK, *L'arte dell'inganno*, Feltrinelli, 2003, p. 15 ss.

[20] Sui rischi legati all'inoculamento fisico del captatore sull'*hardware* bersaglio, v. A. TESTAGUZZA, Digital forensics. *Informatica giuridica e processo penale*, cit., p. 84.

[21] R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., p. 220. Sulle problematiche tecniche, diffusamente, M. ZONARO, *Il* Trojan – *Aspetti tecnici e operativi dell'utilizzo di un innovativo strumento di intercettazione*, cit., p, 166 ss. Sul punto, anche F. PERNA, *Il captatore informatico nell'attuale panorama investigativo*, in *Parola alla difesa,* 2016, f. 1, p. 172, per cui «non solo la fase di studio delle abitudini dell'indagato – indispensabile per la collocazione degli apparati di captazione – potrebbe in prospettiva ridursi in maniera significativa, ma l'esposizione del personale operante, nonché le imprevedibili *discovery* legate alla casualità e allo stesso intervento umano potrebbero essere addirittura eliminate».

flusso informativo del sistema informatico attenzionato, proprio come avviene nel caso di intercettazioni telematiche[22].

In secondo luogo, il maggior consumo di batteria nei dispositivi mobili infettati e l'incremento della banda trasmissiva (a causa della trasmissione dei dati verso il *server* in ascolto), potrebbe insospettire il monitorato e indurlo all'impiego di un differente apparecchio "pulito".

Simili rischi possono essere contenuti adottando opportuni accorgimenti: intanto, si procede all'esportazione dei dati solo allorquando il dispositivo è connesso alla rete *wi-fi* ovvero, se ciò non fosse possibile per ragioni fattuali o per esigenze investigative, si provvede a reintegrare il traffico dati sottratto con la collaborazione dei gestori telefonici.

Non può, tuttavia, sottacersi che un'indagine di questo tipo implichi l'impiego di ingenti risorse tecniche ed economiche, dovendo gli inquirenti avvalersi di apparecchiature sofisticate e competenze specialistiche che, allo stato, sono proprie solo di aziende private che procedono alla creazione e allo sviluppo di simili strumenti.

D'altro canto, l'inoculamento determina frizioni rispetto ai principi fondanti del processo penale: se non si dubita della legittimità dell'inoculazione diretta del captatore da parte dell'operatore di polizia che riesce materialmente a disporre del dispositivo elettronico da infettare, «non è da escludere che possano profilarsi aspetti di criticità in rapporto all'inoculazione occulta, in quanto atto che richiede una cooperazione del soggetto attenzionato che, tuttavia, è *contra se*»[23].

A ben guardare, il principio *nemo tenetur se detegere*[24] non esaurisce la sua portata nella protezione del soggetto interrogato, cui è consentito avvalersi del diritto di autodifesa, espandendo i suoi confini fino a consacrare il precetto per cui «nessuno può

---

[22] Ci si riferisce, in particolare, alla necessità che, dietro compenso, il gestore fornisca all'autorità giudiziaria una linea dati in cui far confluire le informazioni digitali che vedono coinvolto, come mittente o come destinatario, il sistema informatico/telematico bersaglio.

[23] In questo senso S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 238 s. Si tratterebbe, in questi casi, di un'intercettazione «fraudolenta». Così M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 131.

[24] Tale garanzia ha «portata panprocessuale» (P. CORSO, *Diritto al silenzio: garanzia da difendere o ingombro processuale da rimuovere?*, in AA.VV., *Studi in ricordo di Giandomenico Pisapia*, vol. II, Giuffrè, 2000, p. 172), poiché trova applicazione con riferimento a tutti gli atti acquisitivi di dichiarazioni da parte della persona sottoposta a procedimento penale. La matrice dell'incoercibilità del contributo dichiarativo da parte dell'imputato è contenuta nell'art. 64 c.p.p. Rappresenta un imprescindibile punto di riferimento per l'analisi dell'istituto lo studio monografico di V. GREVI, Nemo tenetur se detegere. *Interrogatorio dell'imputato e diritto al silenzio nel processo penale italiano*, Giuffrè, 1972. Sul principio in esame la dottrina è assai copiosa. *Ex multis,* M. BIRAL, *L'identificazione della voce nel processo penale: modelli, forme di accertamento, tutela dei diritti individuali*, in *Riv. it. dir. proc. pen.,* 2015, f. 4, p. 1842 ss.; O. MAZZA, voce *Interrogatorio dell'imputato*, in *Enc. dir*., Annali III, Giuffrè, 2010, p. 712 ss.; F. PETRELLI, *Ad armi pari? le "forme" della "parità" fra costituzione e processo,* in *Cass. pen*., 2019, f. 4, p. 1735 ss. Ma già F. FLORIO, *Il principio* «nemo tenetur se detegere» *e l'accertamento della verità nell'elaborazione dottrinale e giurisprudenziale*, in *Crit. pen.,* 1993, p. 32; G. UBERTIS, *Verso un "giusto processo" penale*, Giappichelli, 1997, p. 68 s. Sotto la vigenza del Codice del 1930, F. CARNELUTTI, *Lezioni sul processo penale,* Edizioni dell'Ateneo, IV ed., 1949, p. 168 ss.; G. FOSCHINI, *Sistema del diritto processuale penale*, Giuffrè, 1968, p. 437*;* A. MACCHIA, voce *Interrogatorio*, in *Noviss. dig. it.,* Appendice, IV, Utet, 1983, p. 328; A. MALINVERNI, *Principi del processo penale*, Giappichelli, 1972, p. 437 s.; G. VASSALLI, *Sul diritto di difesa giudiziaria nell'istruzione penale*, in *Scritti giuridici in onore della Cedam*, vol. II, Cedam, 1953, p. 583.

essere costretto ad agire a proprio danno»[25]. Più in particolare, l'autodifesa può consistere «sia in quell'aspetto attivo rappresentato dalla facoltà per l'imputato di essere presente con le proprie discolpe, senza obblighi di verità, sia in un profilo passivo, inteso come facoltà di difendersi tacendo o, comunque, come facoltà di non fornire elementi in proprio danno»[26]. Così, interpretando in senso più ampio il principio in esame, si potrebbe obiettare che una simile attività, interamente incentrata sulla collaborazione attiva del monitorato, integri una violazione del diritto riconosciuto ad ogni individuo per cui lo stesso non può essere obbligato a compiere azioni che possano ledere la sua persona.

1.1. *SEGUE*: FUNZIONALITÀ E POTENZIALITÀ INVESTIGATIVE

In relazione al dato tecnico, un ultimo aspetto da analizzare inerisce alle in(de)finite potenzialità del captatore; profilo, questo, che incide profondamente sulle logiche processuali, allontanando o avvicinando progressivamente gli esiti delle attività compiute attraverso il «bulimico congegno»[27] alle più o meno note categorie probatorie codificate.

La dottrina maggioritaria tende a distinguere le attività espletabili in due *macro*-aree: le *online search* e *online surveillance*[28].

I programmi spia appartenenti alla prima categoria consentono di far copia, totale o parziale, delle unità di memoria del sistema informatico attenzionato. In particolare, tale tipologia di *software* è tecnicamente in grado di entrare in maniera occulta all'interno del dispositivo "bersaglio" al fine di estrapolare dati e informazioni che, una volta "copiati", vengono trasmessi, in tempo reale o ad intervalli prestabiliti, agli organi di investigazione attraverso un indirizzo Internet prestabilito tramite la rete, in modalità nascosta e protetta.

Attraverso i programmi spia che realizzano la c.d. *online surveillance*, invece, è possibile monitorare il flusso di dati che coinvolgono un determinato sistema informatico o telematico (ora e durata delle connessioni, invio e ricezione di *e-mail, chat*, siti Internet visitati, *files* scaricati, ecc.).

---

[25] Autorevolmente, V. MANZINI, *Trattato, di diritto processuale penale*, VI ed., a cura di G. Conso, vol. II, Utet, 1968, p. 543 s.

[26] O. MAZZA, voce *Interrogatorio dell'imputato*, cit., p. 734.

[27] Lo definisce così L. FILIPPI, L*'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*., 2016, f. 2, p. 349.

[28] In questo senso M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 12 s.; R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., p. 222. Secondo G. ZICCARDI, *Parlamento Europeo, captatore informatico e attività di* hacking *delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche,* in *Arch. pen.,* 2017, f. 1, p. 1, le operazioni tecniche effettuabili per mezzo dell'agente intrusore potrebbero suddividersi in tre macro-aree, riconducibili: 1) al controllo dell'*hardware* del dispositivo; 2) al controllo dei contenuti del dispositivo; 3) all'acquisizioni di informazioni scambiate sul dispositivo. Come precisato, le modalità tecniche per effettuare *online search* o *online surveillance* sono molteplici. Sul punto, esaustivamente, M. HANSEN - A. PFITZMANN, *Techniken der Online Durchsuchung: Gebrauch, Missbrauch, Empfehlungen*, in AA. VV., *Online Durchsuchungen: Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils, Bwv Berliner-Wissenchaft, Auflage,* a cura di F. Roggan, 2008, p. 131 ss.

Tentando di "scomporre" le singole attività esperibili mediante il captatore informatico, può dirsi che il *malware* è in grado di acquisire flussi di comunicazioni tra sistemi informatici e telematici (posta elettronica, messaggistica come *whatsapp*, conversazioni *Voip* come *Skype*), attivare microfono e/o telecamera e rilevatori GPS, registrare tutto quanto digitato sulla tastiera (*keylogging*)[29] e tutto quanto appare sullo schermo (*screenshot*)[30]. Può, inoltre, eseguire attività di *Trojan*, vale a dire entrare nella memoria dei dispositivi in cui sono conservati i dati e, conseguentemente, acquisire tutti i dati e le informazioni *ivi* contenute o transitanti sul dispositivo infettato. Non solo. L'intrusore può essere programmato anche per alterare qualsiasi informazione memorizzata o trasmessa e, di conseguenza, salvare, modificare, cancellare o immettere *file*[31].

Ogni singola attività può essere abilitata a distanza e, analogamente, disabilitata, ma solo dal momento in cui il comando arriva al captatore (ciò vuol dire che può avvenire contestualmente all'invio del comando oppure in maniera ritardata, non appena la linea internet si ripristina). Allo stesso modo, l'esportazione dei dati verso il *server* può non avvenire in tempo reale (per indisponibilità della rete internet), nel quale caso i dati vengono custoditi nell'apparato infettato in attesa della disponibilità d'invio[32].

Proprio dalla sua intrinseca poliedricità derivano le maggiori perplessità dei giuristi: posto che la tecnologia consente di modulare l'impiego del *Trojan* a seconda delle esigenze investigative da soddisfare, al fine di verificare la tenuta degli atti di indagini rispetto all'impianto costituzionale e codicistico, sembra imprescindibile qualificare giuridicamente le attività riconducibili al sistema di controllo da remoto, in modo da individuare la disciplina cui le stesse devono soggiacere.

Come meglio si dirà di seguito[33], la ricerca di una copertura normativa implica, *in primis*, la sussunzione delle attività *de quibus* nell'ambito dei mezzi tipici di ricerca della prova; solo qualora detta ricerca si riveli infruttuosa, occorrerà verificare se l'atto di indagine possa almeno rientrare nella categoria dei mezzi di ricerca della prova atipici.

---

[29] I *keylogger software*, ad esempio, consentono di creare dei *file* di *log* contenenti tutto ciò che viene digitato attraverso la tastiera (fisica o virtuale) del dispositivo. Tale file può essere visualizzato in tempo reale o acquisito in differita, da remoto, da parte del soggetto controllore. In alternativa, gli stessi dati possono essere captati durante la loro trasmissione attraverso uno *sniffer*, ovvero *software* che catturano i pacchetti di informazioni in una rete di computer e possono essere utilizzati per monitorare il funzionamento del sistema e/o scoprire nomi utenti e *passwords*. Così R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, in *Riv. trim. dir. pen. econ.*, 2009, f. 3, p. 695. p. 697.

[30] La questione dell'uso del *trojan* per effettuare *screenshot* è assai delicata in ragione del complesso inquadramento dell'attività dallo stesso scaturente nelle categorie tipiche e atipiche del diritto. Sul punto, esaustivamente, S. ATERNO, *Captatore informatico*, quid iuris *per le modalità* screen shot, in *www.dirittopenaleinformatica.it,* 2017.

[31] Per un'analisi dettagliata delle singole attività esperibili, v. S. ATERNO, *Il punto di vista degli operatori. Il difensore*, in AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 328 s.

[32] In questo senso D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in AA. VV., *Le recenti riforme in materia penale*, a cura di G.M. Baccari-C. Bonzano-K. La Regina- E.M. Mancuso, Wolters Kluwer-Cedam, 2017, p. 560.

[33] Per una disamina approfondita circa l'inquadramento delle attività esperibili dal *virus*, si consenta il rinvio a Cap. II.

In prima approssimazione può ritenersi che l'attivazione del microfono del dispositivo infettato consenta al *malware* di eseguire intercettazioni ambientali, figurando quale nuova tecnica investigativa da impiegare in luogo delle tradizionali microspie (art. 266, comma 2 c.p.p.)[34]. Inoltre, la captazione del flusso di comunicazioni tra sistemi informatici e telematici potrebbe configurare quale intercettazione telematica (art. 266 *bis* c.p.p.); mentre l'accesso al sistema per ricercare tracce e gli altri effetti materiali del reato che possono giacere nella macchina bersaglio ed eventualmente acquisire i *file* di interesse investigativo, è assimilabile alle ispezioni, perquisizioni e sequestri informatici (artt. 244, comma 2, 247, comma 2 *bis*, 253 e 254 c.p.p.)[35].

Tuttavia, una parificazione di questo tipo pare soffrire di un eccessivo semplicismo: fatta eccezione per rare ipotesi e per l'intercettazione che mira esclusivamente all'apprensione di contenuti comunicativi, tutte le altre tipologie investigative tramite captatore sembrano difficilmente riconducibili al catalogo degli atti noti, perché le caratteristiche che potrebbero assimilarli ad essi appaiono sempre cedevoli rispetto ai profili differenziali determinati dalle peculiarità dello strumento tecnico impiegato.

In altri termini, pur potendo superficialmente avvicinare i risultati investigativi ottenuti mediante il captatore informatico a quelli ottenibili mediante l'espletamento di intercettazioni (ambientali e informatiche), delle ispezioni, delle perquisizioni e dei sequestri informatici, le sue stesse potenzialità portano all'esecuzione di atti di indagine completamente inediti che assommano le caratteristiche proprie dei mezzi di ricerca della prova tipici[36].

Sostanzialmente, gli esiti fattuali del *Trojan* sono così ampi e complessi da delineare figure probatorie amorfe, non normate dal legislatore contemporaneo, sfociando (tutt'al più) in strumenti di esecuzione di mezzi di ricerca della prova atipici[37].

---

[34] Unica attività normata dal legislatore contemporaneo. Gli aspetti tecnici relativi all'uso del captatore per le intercettazioni di comunicazioni tra presenti, introdotti dal d.lgs. 29 dicembre 2017, n. 216, recante "*Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017,* n. 103", in *Gazz. uff.,* 11 gennaio 2018, n. 8, saranno presi in esame *infra*, § 5.

[35] In argomento, in particolare, R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Arch. pen.,* 25 luglio 2016.

[36] In questo senso, L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in Arch. pen., 2016, f. 2, p. 349 s. Si consenta, inoltre, il rinvio a W. NOCERINO, *Il captatore informatico: un giano bifronte. Prassi operative* vs *risvolti giuridici*, in *Cass. pen.,* 2020, f. 2, p. 826. Come evidenziano L. CUOMO-L. GIORDANO, *Informatica e processo penale*, in *Proc. pen. giust*., 2017, f. 4, p. 729, «[…] le poliedriche funzioni del captatore informatico rendono persino poco agevole capire cosa si è fatto in concreto».

[37] In questo senso F. GIUNCHEDI, *Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?,* cit., p. 134. Si è molto discusso circa la possibilità di ammettere mezzi di ricerca della prova atipici. Parte di dottrina rileva l'impossibilità di estendere la portata dell'art. 189 c.p.p. anche ai mezzi di ricerca della prova esperiti nel corso delle indagini, in quanto si tratta di prove che sono precostituite rispetto all'istruzione dibattimentale e che, di norma, vengono acquisite a sorpresa. Non sarebbe, quindi, possibile dare completa attuazione all'art. 189 c.p.p., nella parte in cui impone che il giudice senta le parti sulle modalità di assunzione della prova, prima di decidere con ordinanza sulla richiesta di ammissione. Così N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992, p. 213. La dottrina maggioritaria propende, tuttavia, per «un'interpretazione elastica» dell'art. 189. Sembrano orientarsi in questo senso le sezioni Unite della Cassazione. Cfr. Cass., sez. un., 28 luglio 2006, n. 26795, in *Arch. nuova proc. pen.*, 2006, f. 6, p. 621 ss., in cui la Corte Suprema ha provveduto a distinguere tra mezzo di ricerca, elemento e mezzo di prova: «[..]il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova, ma la sua

In particolare, l'accesso al sistema per la ricerca di tutti dati utili alle indagini pur non essendo strettamente connessi alla repressione del reato determina un'intrusione a fini esplorativi (c.d. perquisizioni *online*)[38] che, come evidenziato, «è […] assai più invasiva di un'intercettazione, dato che mentre in quest'ultima ipotesi si capta il contenuto comunicativo che un soggetto ha comunque deciso di rivelare al suo interlocutore, nel caso della visualizzazione dei contenuti digitali si può invadere la sfera più riservata di una persona»[39], potendo determinare una lesione «all'inviolabilità della psiche»[40]. Inoltre, consentendo l'attivazione della videocamera eventualmente collocata sul dispositivo, il captatore può compiere videoriprese investigative al fine di effettuare un monitoraggio costante dei comportamenti della persona sottoposta a indagine, comunicativi e non, in ogni momento e in qualsiasi luogo si trovi[41]; l'attivazione del GPS satellitare dell'apparato mobile realizza una forma di pedinamento tecnologico avanzato, "mappando" ogni spostamento del soggetto attenzionato. Infine, l'ipotesi che il *Trojan* venga abilitato ad un'apprensione generale di tutto ciò che viene digitato sulla tastiera dell'indagato e di tutto quanto compare sullo schermo del dispositivo infettato – anche di testi di tipo comunicativo – sembra di difficile inquadramento se non sul piano dell'atipicità.

Anche la prospettiva per cui il captatore informatico possa rappresentare uno strumento tramite il quale realizzare perquisizioni *online* – e, dunque, allocarlo nell'ambito dei mezzi di ricerca della prova atipici - non può essere accolta senza riserve: per evitare censure di incostituzionalità, infatti, anche le categorie probatorie non tipizzate

---

assunzione e interviene, dunque, come risulta chiaramente dalla disposizione, quando il giudice è chiamato a decidere sull'ammissione della prova». In dottrina v. A. SCALFATI, *Premesse sulla prova penale*, in AA. VV*., Trattato di procedura penale,* a cura di A. Scalfati, diretto da G. Spangher, vol. 1, Utet, 2009, p. 32 ss.; D. SIRACUSANO, *Le prove*, in AA. VV., *Diritto processuale penale*, Giuffrè, 2011, p. 399. In quest'ultimo caso, anziché utilizzare un contraddittorio anticipato circa l'ammissione, si potrebbe svolgere un contraddittorio successivo circa l'utilizzabilità degli elementi acquisiti. Così A. CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionale*, in *Cass. pen.,* 1999, f. 9, p. 1195 s.; L. FILIPPI, L'home watching*: documento, prova atipica o prova incostituzionale?,* in *Dir. pen. proc*., 2001, f. 1, p. 92; G. F. RICCI, *Le prove atipiche*, Giuffrè, 1999, p. 538 ss. Sulla dibattuta questione legata alla sussistenza di una simile categoria probatoria, con specifico riferimento alle attività condotte mediante captatore informatico, si rinvia a Cap. II, § 5.

[38] Sul punto, esaustivamente, L. PARLATO, voce *Perquisizioni on-line,* in *Enc. dir.,* Annali, vol. X, Giuffrè, 2017, p. 603 ss. Ma già S. MARCOLINI, L*e cosiddette perquisizioni on line (o perquisizioni elettroniche),* in *Cass. pen.,* 2010, f. 7-8, p. 2855 ss.; M. TROGU, *Sorveglianza e "perquisizioni"* on-line *su materiale informatico*, I ed., cit., p. 431.

[39] L'espressione appartiene a S. SIGNORATO, *Le indagini digitali. Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 292

[40] Così P. TONINI-C. CONTI, *Il diritto delle prove penali*, Giuffrè, 2014, p. 482.

[41] In dottrina v. S. BELTRANI, L*e videoriprese? Sono una prova atipica ma le Sezioni unite non sciolgono il nodo,* in *Dir. e giust*. 2006, p. 34 ss.; C. CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati",* in *Dir. pen. proc*., 2006, f. 11, p. 1347 ss.; L. PULITO, *Più garanzie per le videoriprese nel "quasi domicilio",* in *Arch. nuova prc. pen.,* 2007, f. 4, p. 494 ss.; F. RUGGIERI, *Riprese visive e inammissibilità della prova*, in *Cass. pen*., 2006, f. 12, p. 3937 ss. Le videoriprese in luoghi pubblici o aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria di documenti, *ex* art. 234 c.p.p. Cfr. Cass., sez. VI, 17 novembre 2009, n. 36083, in *Guida dir*., 2010, f. 1, p. 90 ss.

devono garantire la tutela dei diritti inviolabili della persona[42], quali l'art. 13 Cost., baluardo della libertà di ogni individuo, l'art. 14 Cost., posto a protezione del domicilio, l'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, nonché il principio di proporzionalità che impone, ai sensi dell'art. 8 CEDU, la necessità di una perfetta corrispondenza tra i risultati perseguiti e i mezzi adoperati e, più in particolare, tra la potenziale forza invasiva del mezzo in esame e l'inevitabile lesione dei diritti fondamentali[43].

Come evidenziato dalla giurisprudenza[44] e dalla dottrina[45], con il captatore informatico è possibile svolgere (anche contemporaneamente) un'eterogenea congerie di attività tipiche e atipiche di indagine pesantemente intrusive delle libertà del soggetto destinatario, eziologicamente volte, come una sorta di "*panopticon* benthamiano", a sorvegliare ogni atto quotidiano della vita[46]; «la valenza intrusiva del captatore è elevatissima, potendo esso effettuare contemporaneamente un'intercettazione ambientale, telematica, effettuare riprese audio e video, una geolocalizzazione, un appostamento e un pedinamento informatico, rastrellando una grande quantità di dati e immagini tratti dall'ambiente circostante»[47].

Ci si trova, dunque, difronte ad uno strumento onnivoro[48], atto a realizzare forme di controllo assai pervasive e, proprio per tale ragione, di "spiccata invadenza"[49], tali da rendere pienamente comprensibili gli interrogativi da parte di chi sottolinea il potenziale

---

[42] *Ex multis*, P. FELICIONI, L*e fattispecie "atipiche" e l'impiego processuale*, cit., p. 315 ss.; ID., *L'acquisizione da remoto di dati digitali nel procedimento* penale: *evoluzione giurisprudenziale e prospettive di riforma,* cit., p. 7; F. GIUNCHEDI, *Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?,* in *Proc. pen. giust*, 2014, p. 133 ss.; S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia,* 2006, p. 387 ss.

[43] Invero, il catalogo dei diritti potenzialmente compressi con l'attività investigativa *de qua* è assai più ampio e complesso. Sull'incidenza delle attività condotte mediante captatore sui diritti fondamentali si rinvia a Cap. IV.

[44] Cass., sez. un., 28 aprile 2016, n. 26889, in *Arch. pen*., 2016, f. 2, p. 348 ss.

[45] S. ATERNO, voce Digital forensics *(investigazioni informatiche),* cit., p. 217 ss.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 483 ss.; D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, cit., p. 385; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 45 ss.; L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* in *Dir. pen. cont.*, 2017, f. 3, p. 177 ss.; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont*., 2018, f. 1, p. 216; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 239; A. TESTAGUZZA, *I sistemi di controllo da remoto: tra normativa e prassi*, *cit.,* p. 759 ss.; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 18.

[46] Come sostenuto, «[A]ppare riduttivo, ma scontato, l'inquadramento del captatore informatico come strumento tecnico dell'intercettazione». In questo senso M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont*., 20 dicembre 2018.

[47] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[48] W. NOCERINO, *Il captatore informatico: un giano bifronte. Prassi operative* vs *risvolti giuridici*, cit., p. 828.

[49] Così C. PELOSO, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo,* in *Dir. pen. cont*., 2017, f. 1, p. 150.

grave *vulnus* alle garanzie fondamentali dei singoli, derivante da un utilizzo non rigidamente regolamentato di tale forma captativa[50].

2. IL *VIRUS* DI STATO NELLA GIURISPRUDENZA DI LEGITTIMITÀ: DA ARNESE PER LE INVESTIGAZIONI "*AD EXPLORANDUM*" A STRUMENTO DI INTERCETTAZIONE "AMBIENTALE"

Si esaurisce in un decennio la *querelle* legata all'introduzione del captatore informatico nel circuito del processo penale. Il percorso è stato lento e tortuoso e ha visto la giurisprudenza brancolare nel buio dell'inedito mondo tecnologico: pronunce intermittenti e contraddittorie, hanno consacrato il definito ingresso del *Trojan* nelle logiche processuali, qualificandolo talvolta come prova atipica (*ex* art. 189 c.p.p.)[51], talaltra quale nuovo strumento di indagine per dare attuazione a mezzi di ricerca della prova tradizionali (artt. 266 ss. c.p.p.)[52].

Prima di imbatterci nei discutibili orientamenti giurisprudenziali, sembra doverosa una precisazione di carattere generale. A prescindere dai diversi approdi raggiunti dalle singole pronunce, i giudici di legittimità peccano di essere stati "miopi" e inavveduti nel non interrogarsi sull'effettiva collocazione del complesso di attività espletabili mediante il *virus* informatico e quando il legislatore è troppo attento a inseguire le questioni giurisprudenziali, rischia di smarrire la visione d'insieme.

Sarebbe stato preferibile un approccio olistico funzionale a chiarire il parametro normativo di riferimento più adeguato alla portata dello strumento, andando oltre il caso sottoposto alla loro attenzione. In altri termini, la Suprema corte si limita a qualificare di volta in volta l'atto compiuto dal captatore informatico solo in relazione alla fattispecie concreta affrontata, mentre nessun cenno viene fatto alle altre attività che, almeno in potenza, il diabolico strumento è in grado di compiere[53].

Di qui, i dubbi esegetici della dottrina in ordine sia alla legittimità dei risultati investigativi scaturenti dalle "altre" funzioni del *virus*, sia in relazione alla cornice normativa di riferimento[54].

---

[50] Sul tema, *ex multis*, A. CAPONE, *Intercettazioni e costituzione*. *Problemi vecchi e nuovi*, in *Cass. pen*., 2017, f. 3, p. 1263 ss.; O. MAZZA, *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, in *Proc. pen. giust*., f. 4, p. 684 ss.; M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in *Dir. pen. cont*., 2018, n. 2, p. 43; P. P. RIVELLO, *Le intercettazioni mediante captatore informatico* cit., p. 105; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 69; G. SILVESTRI, *L'individuazione dei diritti della persona*, Relazione presentata al XXXII Convegno dell'Associazione tra gli studiosi del processo penale "Prof. G.D. Pisapia", intitolato "*Diritti della persona e nuove sfide del processo penale",* tenutosi a Salerno dal 25 al 27 ottobre 2018, in *Dir. pen. cont.,* 29 ottobre 2018, p. 8 s.; G. SPANGHER, Le *criticità della disciplina delle intercettazioni telefoniche*, in *Dir. pen. proc.,* 2016, p. 921 ss.

[51] Cass., sez. VI, 27 novembre 2012, n. 15009, in *C.E.D. Cass*., n. 254865; sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.,* n. 246954.

[52] Cass., sez. VI, 12 marzo 2015, n. 24237, inedita; sez. VI, 8 aprile 2015, n. 27536, inedita; sez. VI, 26 maggio 2015, n. 27100, in *Guida dir.,* 2015, f. 41, p. 83 s.

[53] Condivide la medesima impostazione M.T. ABBAGNALE, *In tema di captatore informatico*, cit., p. 8.

[54] Sul punto si consenta un rinvio a Cap. II, § 1.

Una delle prime pronunce in materia vede i giudici di legittimità ricondurre il captatore informatico alla categoria delle prove atipiche, sulla base dell'assunto per cui l'attività di indagine si è fondata sulla mera copia di documenti memorizzati nell'*hard disk* dell'apparecchio in uso all'indagato[55].

Il "caso" trae origine da un'inchiesta in materia di associazione a delinquere di stampo mafioso dedita alla commissione, tra gli altri, di delitti contro la pubblica amministrazione, nel corso della quale la Polizia di Stato utilizza un *software* tipo *Trojan*[56] al fine di acquisire i *files* contenuti nella memoria di un computer collocato presso un ufficio pubblico.

La prima anomalia si riscontra nella scelta del p.m. di autorizzare l'esecuzione delle operazioni con un decreto di acquisizione di atti, ai sensi dell'art. 234 c.p.p., dal momento che lo strumento ha consentito la registrazione non solo dei *files* già esistenti nel sistema, ma di tutti quelli *elaborandi*, ossia anche dei dati inseriti immessi successivamente nel dispositivo, innescando in tal modo un monitoraggio da remoto occulto e continuativo del sistema informatico.

La collocazione delle attività esperite mediante captatore nel *genus* della prova atipica, nonostante le incisive riserve della difesa - sostenitrice della necessaria sussunzione delle attività investigative nell'alveo delle intercettazioni telematiche (art. 266 *bis* c.p.p.)[57] - , trova conferme sia in appello che in Cassazione, la quale riconduce l'attività del captatore alle *on line search*[58], «tralasciando l'altro segmento di indagine in concreto realizzatosi»[59].

In particolare, secondo la Corte, la captazione dei dati (sia memorizzati che *elaborandi*) non può costituire un'intercettazione telematica *ex* art. 266 *bis* c.p.p., in quanto la registrazione non avrebbe avuto ad oggetto «un flusso di comunicazioni»[60] -

---

[55] Cass., sez. V, 14 ottobre 2009, n. 16556, cit. Per commenti, M.T. ABBAGNALE, *In tema di captatore informatico*, cit., p. 2 s.; S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.; ID., *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, cit., p. 7.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, cit., p. 8; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 128; L. GIORDANO, *La disciplina del "captatore informatico"*, in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci, 2018, p. 250; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 314 s.; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 932 s.; ID., *Exitus acta probat "Trojan" di Stato: la composizione di un conflitto,* in *Arch. pen.,* 2016, f. 2, p. 9 ss.

[56] All'epoca probabilmente fu utilizzato un *software* dal nome "*Back Orifice*", le cui potenzialità sono sconosciute anche agli operatori.

[57] In particolare, la difesa con i motivi di appello aveva eccepito che il predetto decreto del p.m., pur autorizzando la mera acquisizione in copia degli atti, avrebbe costituito di fatto la premessa per condurre un'attività di intercettazione si comunicazioni informatiche ai sensi degli artt. 266 *bis* ss. c.p.p.

[58] In questo senso A. BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea,* cit., p. 2276, il quale sottolinea che si tratta di una sentenza relativa alle *on line search.*

[59] Così P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 128.

[60] In quella sede, i Giudici hanno anche specificato cosa debba intendersi con la suddetta locuzione: «la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente

che presuppone un dialogo con altri soggetti - ma «una relazione operativa tra microprocessore e video del sistema elettronico» ovvero «un flusso unidirezionale di dati». Pertanto, l'attività di captazione in questione viene ricondotta nel concetto di prova atipica, escludendo la violazione della disciplina di cui all'art. 189 c.p.p., dal momento che la mancata acquisizione in contraddittorio della prova documentale estrapolata dal computer è determinata dalla specialità del rito scelto dalla difesa e la prescrizione che impone al giudice di procedere in contraddittorio tra le parti riguarda l'assunzione delle fonti di prova e non dei mezzi di ricerca della prova[61].

D'altra parte, a parere della Corte nessuna violazione può ricontrarsi in relazione al dettato costituzionale di cui agli artt. 14 e 15 Cost.

Quanto alla prima disposizione, la Corte ne esclude la violazione dal momento che «l'apparecchio monitorato con l'installazione del captatore informatico non era collocato in un luogo domiciliare o in un luogo di privata dimora, ma nei locali sede di un ufficio comunale, dove l'imputato non godeva di uno *ius excludendi alios*»[62].

---

ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici […]». Così Cass., sez. V, 14 ottobre 2009, n. 16556, cit. Sulla nozione di "flusso di comunicazioni" si veda anche Cass., sez. un., 23 febbraio 2000, n. 6, in *Cass. pen.,* 2000, f. 12, p. 3245 ss. Come rileva la dottrina l'introduzione di programmi spia risulta essere «totalmente estranea alla funzione descrittiva, tipicamente statica, delle ispezioni, essendo atto ad una "subdola" raccolta, anche prolungata nel tempo, di dati e informazioni di pertinenza dell'indagato, a sua insaputa». Così S. MARCOLINI, *Le cosiddette perquisizioni* online *(o perquisizioni elettroniche),* cit., p. 2855.

[61] In questo senso, S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, cit., p. 7.

[62] In base all'evoluzione giurisprudenziale, può dirsi che i luoghi "domiciliari" sono quei luoghi in cui il titolare possiede uno *ius excludendi alios* stabile, ovvero azionabile anche quando il soggetto non sia fisicamente presente. Come precisato, il carattere di "stabilità" del diritto risulta, ai fini della determinazione del concetto di domicilio, assolutamente necessario. Rientrano, pertanto, nella nozione di domicilio solo i luoghi che assolvono in concreto alla finalità di proteggere la vita privata del loro possessore, durante lo svolgimento delle sue attività professionali, di svago, di alimentazione, di riposo. In questo senso, G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione*, in AA. VV., *Le nuove intercettazioni*, cit., p. 139 s. Detto in altri termini, affinché scatti la protezione prevista da tale articolo, non basta che un comportamento venga tenuto in un luogo di privata dimora, in quanto occorre che esso sia in concreto riservato, e, cioè non possa in concreto essere liberamente osservato dagli estranei, senza ricorrere a particolari accorgimenti. Cfr. Corte cost., 7 maggio 2008, n. 149, in *Cass. pen*., 2008, f. 12, p. 4109. Seguendo un simile filone interpretativo, può sostenersi che è considerato domicilio un ufficio privato (Cass., sez. VI, 29 settembre 2003, n. 4933, in *Cass. pen*., 2005, f. 10, p. 1336), mentre non sono tali le stanze di un ospedale (sez. V, 11 ottobre 2018, n. 5300, in *C.E.D. Cass.,* n. 27592) o le celle carcerari (sez. VI, 15 maggio 2018, n. 26028, *ivi*, n. 273417), il pianerottolo di un'abitazione privata (sez. 5, 30 maggio 2017, n. 34151, *ivi,* n. 270679), il *box* cassa di un'autorimessa (sez. V, 17 novembre 2015, n. 11419, in *Cass. pen*., 2017, f. 2, p. 722 ss., con nota di C. RIZZO, *Videoregistrazioni domiciliari e l'incerta distinzione tra comportamenti comunicativi e non)*. Sul punto, V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa,* in *Proc. pen. giust*., 2019, f. 2, p. 336 ss. In proposito la giurisprudenza della Suprema corte ha, ormai, disposto che l'autovettura non può essere considerata un luogo di "privata dimora", in quanto quest'ultima è destinata al trasporto «di persone o al trasferimento di oggetti da un luogo ad un altro ed in quanto sfornito dei confort minimi per potervi risiedere stabilmente per un apprezzabile lasso di tempo [...]» Così sez. I, 6 maggio 2008, n. 32851, in *Cass. pen*., 2009, f. 8, p. 2533. Da ultimo, sez. VI, 30 gennaio 2019, n. 23819, in *C.E.D. Cass.,* n. 275994. La delicata *quaestio* sembra aver trovato una stabilità

In relazione al secondo aspetto, nemmeno può essere invocata la tutela costituzionale della riservatezza della corrispondenza e in genere delle comunicazioni (art. 15 Cost.), giacché quanto riprodotto in copia, non era un testo inoltrato e trasmesso con il sistema informatico privato e personale ma «soltanto predisposto per essere stampato su supporto cartaceo e successivamente consegnato sino al suo destinatario».

Come già in precedenza accennato, il *punctum dolens* della pronuncia in esame risiede non tanto nell'inquadramento giuridico dell'acquisizione mediante captatore nel *genus* della prova atipica[63], quanto nell'aver vagliato la compatibilità con il sistema costituito della sola attività espletate dal *Trojan* nel caso di specie, evitando un approccio olistico – sicuramente "scomodo" ma – funzionale a dare risposte di più ampio spessore.

La linea interpretativa della sentenza "Virruso", trova conferme in una successiva pronuncia[64]. Si tratta del c.d. "caso Bisignani" inerente ad un'indagine per una presunta associazione di stampo massonico P4, avviata dalla Procura della Repubblica presso il Tribunale di Napoli. Secondo il p.m. gli imputati avrebbero instaurato, grazie ad un'intricata rete di influenti amicizie, un sistema informativo parallelo con l'obiettivo di procedere «[…] ad un'illecita acquisizione di notizie e di informazioni, anche coperte da segreto, alcune delle quali inerenti a procedimenti penali in corso nonché di altri dati sensibili o personali al fine di consentire a soggetti inquisiti di eludere le indagini giudiziarie ovvero per ottenere favori o altre utilità». Di qui, la necessità di procedere all'acquisizione occulta di informazioni mediante un *virus* informatico istallato nei dispositivi elettronici in uso agli imputati. Seppur l'autorità inquirente chiede al giudice per le indagini preliminari l'emissione di un decreto autorizzativo ai sensi dell'art. 266 c.p.p., il giudicante emana tale provvedimento solo con riferimento all'attività assimilabile alle intercettazioni; rispetto alle altre investigazioni, facendo espressamente riferimento al precedente giurisprudenziale, ritiene che un provvedimento del pubblico ministero (*ex* art. 234 c.p.p.) sia sufficiente a tutelare le esigenze di riservatezza dei soggetti interessati.

---

ermeneutica grazie al recente apporto delle sezioni unite che accoglie un'interpretazione maggiormente restrittiva alla nozione *de qua*. Cfr. Cass., sez. un., 23 marzo 2017, n. 31345, in *Dir. pen. cont*., 2017, f. 7/8, con nota di S. BERARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624* bis *c.p.,* secondo cui «rientrano nella nozione di privata dimora di cui all'art. 624 *bis* c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare». Per una ricostruzione storica della nozione di privata dimora v. L. FILIPPI, sub *art. 226*, in *Codice di procedura penale commentato*, a cura di A. Giarda-G. Spengher, Wolters Kluwer, 2017, p. 2541 ss.

[63] Come osservato, «l'attività di captazione da remoto attraverso un *software trojan* autorizzato dal pubblico ministero non è un'intercettazione di comunicazioni informatiche o telematiche e in questo caso ha avuto ad oggetto un computer situato presso un ufficio pubblico (non è luogo di privata dimora)». Così S. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, cit., p. 7.

[64] Cass., sez. VI, 27 novembre 2012, n. 15009, cit. Per una disamina della pronuncia in esame, M.T. ABBAGNALE, *In tema di captatore informatico*, cit., p. 3 s.; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma,* cit., p. 128; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 933; M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.,* 2015, f. 9, p. 1163.

A ben guardare, la pronuncia in esame si profila ancor più assai critica rispetto al precedente caso vagliato dalla Suprema Corte, dal momento che il captatore informatico, nel caso concreto, ha proceduto sia ad acquisire ed estrapolare dati e informazioni digitali memorizzati nella memoria di massa del sistema informatico bersaglio, sia a realizzare una vera e propria intercettazione ambientale prendendo il controllo occulto del microfono e della *webcam* dell'elaboratore.

Dopo una fase di stallo, negli anni immediatamente a ridosso dalla fatidica pronuncia delle Sezioni unite[65], si sviluppa un'elaborazione giurisprudenziale che, convenzionalmente, può essere. articolata in tre fasi.

Va preliminarmente chiarito che si tratta di pronunce accomunate dal riferimento a giudizi *de libertate* relativi a reati di criminalità organizzata per i quali erano state emesse ordinanze di custodia cautelare fondate essenzialmente su indagini, riferibili all'*on line surveillance,* effettuate mediante programmi spia inseriti in alcuni dispositivi in uso agli indagati; in tutti i casi la Suprema Corte attrae l'indagine informatica nell'alveo delle intercettazioni ambientali (art. 266, comma 2 c.p.p.).

In una prima fase, la giurisprudenza di legittimità dichiara infondate le censure ai provvedimenti cautelari sia per ragioni di rito attinenti alla genericità dei motivi, sia evidenziando le implicazioni della disciplina speciale relativa alle intercettazioni nei procedimenti di criminalità organizzata[66]. In particolare, si afferma che la censura relativa alla mancanza di motivazione che nei luoghi di privata dimora, oggetto di intercettazione ambientale, si stesse svolgendo l'attività criminosa è infondata poiché le captazioni sono state disposte ai sensi dell'art. 13 d.l. 13 maggio 1991, n. 152 conv. con modificazioni in l. 12 luglio 1991, n. 203 che, testualmente, prescinde da tale requisito, in quanto prevede che l'intercettazione di comunicazione tra presenti è consentita anche in assenza del suddetto presupposto[67].

---

[65] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[66] Cass., sez. VI, 12 marzo 2015, n. 24237, cit.; sez. VI, 8 aprile 2015, n. 27536, cit. Sul tema, P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 129.

[67] *Ex* art. 13, d.l. 13 maggio 1991, n. 152, recante "*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*", in *Gazz. uff.,* 13 maggio 1991, n. 110, convertito, con modificazioni, in l. 12 luglio 1991, n. 203, in *Gazz, uff.*, 12 luglio 1991, n. 162. Per i reati di criminalità organizzata e terrorismo, la norma prevede dei requisiti "attenuati" rispetto a quelli tradizionali: le intercettazioni tra presenti possono essere condotte anche nel domicilio a prescindere dal «fondato motivo di ritenere che in quel luogo si stia consumando un'attività criminosa»; l'intercettazione è ammessa sulla basi di «sufficienti indizi» (e non gravi, *ex* art. 267 c.p.p.), quando la stessa è «necessaria» (e non indispensabile *ex* art. 267 c.p.p.) alla prosecuzione delle indagini; la durata delle operazione non può superare i 40 giorni, prorogabili di 20. Di qui, per i reati "gravi" non contemplati dagli artt. 51, commi 3 *bis* e 3 *quater*, richiamati dall'art. 266, comma 2 *bis* c.p.p., sono ammesse le intercettazioni ambientali domiciliari senza alcun limite se si tratta di captazioni "tradizionali"; viceversa, se le stesse sono eseguite mediate captatore, soggiacciono al requisito di cui al comma 2 dell'art. 266. Inoltre, è per questi previsto l'obbligo di motivazione "rafforzata" con l'indicazione dei tempi e dei luoghi della captazione, secondo il disposto dell'art. 267, comma 1 c.p.p. Sul tema, per tutti, D. MANZIONE, *Una normativa "d'emergenza" per la lotta alla criminalità organizzata e la trasparenza e il buon andamento dell'attività amministrativa (d.l. 152/1991 e l. n. 203/1991): uno sguardo d'insieme*, in *Legislaz. pen*., 1992, p. 852 ss. La normativa viene progressivamente ampliata, ai sensi dell'art. 3 del d.l. 18 ottobre 2001, n. 374, recante "*Disposizioni urgenti per contrastare il terrorismo internazionale*" ai procedimenti per i delitti di cui all'art. 270 *ter* c.p.p. e ai delitti delineati dall'art. 407, comma 1, lett. a), n. 4 c.p.p., nonché ai delitti

Il *renvirement* della Suprema Corte alla fine del 2015 segna l'inizio di una nuova era per il *virus* di Stato, demonizzato e stigmatizzato quale prova incostituzionale[68].

La questione concerne l'utilizzabilità di un agente intrusore come inedito strumento di indagine, al fine di captare conversazioni e comunicazioni, *ex* artt. 266 ss. c.p.p. (attraverso l'attivazione del microfono del dispositivo infettato) ed effettuare videoriprese investigative (attivando anche la videocamera dell'apparato).

In quella circostanza, la Corte stabilisce che l'intercettazione da remoto di conversazioni tra presenti mediante l'attivazione impiegando il c.d. agente intrusore, del microfono di un apparecchio telefonico *smartphone*, vada ricondotta alla categoria delle intercettazioni ambientali (art. 266, comma 2 c.p.p.), ma non senza riserva. Infatti, i giudici precisano che «[N]non si tratta […] di una semplice modalità attuativa del mezzo di ricerca della prova, costituito dalle intercettazioni. Si tratta, invece, di una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un *quid pluris* rispetto alle ordinarie potenzialità dell'intercettazione […]», dal momento che le intercettazioni mediante captatore informatico consentono di captare le conversazioni tra presenti in una varietà di luoghi, a seconda degli spostamenti del soggetto che ha in uso il dispositivo infestato dal *virus Trojan*.

Di qui, secondo i giudici della Suprema Corte, sarebbero legittime le intercettazioni ambientali condotte attraverso l'impiego del captatore informatico, installato su un dispositivo elettronico, purché l'attività avvenga nel rispetto dei limiti imposti dal decreto autorizzativo dell'autorità giudiziaria, ai sensi dell'art. 267 c.p.p.[69]: non sono, di

---

di cui agli artt. 270, comma 3 e 306, comma 2 c.p.p. Inoltre, l'art. 9 l. 11 agosto 2003, n. 228 estende l'applicazione delle disposizioni di cui all'art. 13 d.l. 13 maggio 1991, n. 152, in relazione ai procedimenti per i delitti previsti dal libro II, titolo XII, capo III, sez. I c.p. (al netto delle ipotesi ricomprese nell'art. 51, comma 3 *bis*, c.p.p.), nonché a quelli previsti dall'art. 3, l. 20 febbraio 1958, n. 75. Limitandoci ai lavori di carattere più generale, E. APRILE, *Intercettazioni di comunicazioni,* in AA. VV., *Trattato di procedura penale,* t. 1, v. 2, a cura di A. Scalfati, diretto da G. Spangher, Utet, 2009, p. 475 ss.; E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuovi questioni giuridiche*, Giuffrè, 2004, p. 108 ss.; P. BALDUCCI, *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria,* Giuffrè, 2002; A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996; L. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, 1997; ID., *Intercettazione,* in AA. VV., *La prova penale,* a cura di P. Ferrua–E. Marzadura– G. Spangher, Giappichelli, 2013, p. 837; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007; D. SIRACUSANO–F. SIRACUSANO, *Le prove*, in AA. VV., *Diritto processuale penale*, a cura di G. Di Chiara–V. Patanè–F. Siracusano, Giuffrè, 2018, p. 318 s.; C. PARODI, *Le intercettazioni. Profili operativi giurisprudenziali*, Giappichelli, 2002, p. 88 ss.

[68] Cass., sez. VI, 26 maggio 2015, n. 27100, cit. Per approfondimenti si rinvia a M.T. ABBAGNALE, In tema di captatore informatico, cit., p. 4 s.; G. AMATO, Intercettazioni mediante agenti intrusori: la Cassazione non è al passo con i tempi, in *Guida dir.,* 2015, n. 41, p. 83 ss.; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 106; *indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 237 ss.; A. TESTAGUZZA, voce Virus *informatico*, cit., p. 934

[69] Si richiede, infatti, che l'attività captativa, non potendosi svolgere «ovunque», debba avvenire entro i limiti imposti dal provvedimento motivato del giudice, sempre nel rispetto della riservatezza. La Corte Suprema «annulla l'ordinanza impugnata e rinvia per nuovo esame al Tribunale di Catania», in modo da verificare che «i decreti autorizzativi contenessero una precisa individuazione dei luoghi cui procedere ad intercettazione ambientale e che non siano state effettuate in luoghi diversi da quelli ai quali si riferiva l'autorizzazione […], e che, mediante l'attivazione da remoto della telecamera inerente al telefono cellulare, non siano state effettuate videoregistrazioni all'interno dei luoghi di privata dimora o, comunque, tali da imporre la necessità di tutelare la riservatezza personale […]». Cfr. sez. VI, 26 maggio 2015, n. 27100, cit.

conseguenza, consentite, in virtù di una «corretta ermeneutica dell'art. 15 Cost.», intercettazioni ambientali effettuate "ovunque", senza limitazioni di luoghi in cui l'attività possa essere espletata.

Su un altro versante, l'attivazione, da remoto, della videocamera del telefono cellulare, consentirebbe di effettuare videoriprese di comportamenti non comunicativi[70] anche nell'ambito domiciliare[71], che, ai fini processuali, risultano essere inutilizzabili, in quanto acquisite illecitamente[72]. Di qui, «[L]le videoriprese effettuate mediante l'attivazione attraverso il c.d. *virus* informatico della telecamera di un apparecchio telefonico *smartphone*, possono ritenersi legittime quali prove atipiche ai sensi dell'art. 189 c.p.p., salvo che siano effettuate all'interno di luoghi di privata dimora […]».

La terza e ultima fase dell'elaborazione giurisprudenziale in considerazione si riferisce ad una pronuncia del 2016, con cui la Suprema Corte[73], prendendo le distanze dalla precedente sentenza del 2015[74] ed evidenziando la sussistenza di un contrasto difficilmente sanabile, rimette alla Sezioni Unite tre differenti questioni nelle quali esaurisce il ventaglio delle situazioni giuridiche percorribili: escludere in toto l'utilizzabilità dei risultati dell'attività condotta a mezzo di *virus Trojan* in mancanza dei requisiti degli artt. 266 ss. c.p.p., escludere solo le captazioni effettuate nei luoghi di

---

[70] «La nozione di comunicazione consiste nello scambio di messaggi tra più soggetti, in qualsiasi modo realizzate (ad esempio tramite colloquio orale o anche gestuale […]». Sul punto cfr. Cass., sez. IV, 19 gennaio 2005, n. 11181, in *C.E.D. Cass.,* n. 231047.) Nozione del tutto differente dall'usuale azione intercettativa sopra descritta, è quella di «captare immagini relative alla mera presenza di cose o persone o ai loro movimenti, non funzionali alla captazione di messaggi». Cfr. Sez. VI, 10 novembre 1997, n. 4397, in *Cass. pen.,* 1999, f. 10, p. 1188 ss. Si può notare come nella prima fattispecie lo scopo è quello di percepire sul piano uditivo ed interpretativo conversazioni, onde inferire da essi contenuti illeciti e, dunque, facilmente inquadrabile nella disciplina delle intercettazioni ambientali (artt. 266 ss.), con tutti i limiti ad esse imposte dal codice di rito.

[71] Sul concetto di "luogo di privata dimora, v. *supra* nt. 61.

[72] Cass., sez. un., 28 luglio 2006, n. 26795, cit. Per un approfondimento sull'uso del *trojan* per condurre videoriprese anche nell'ambito domiciliare, cfr. Cap. II, § 6.3.

[73] Cass., sez. VI, 10 marzo 2016, n. 13884, in *Dir. inf. e informatica*, 2016, n. 1, p. 81, con nota critica di G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali.* Sul tema, anche M.T. ABBAGNALE, *In tema di captatore informatico,* cit., p. 5 ss.; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 129; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 107 s.

[74] Era stato inoltrato un ricorso in Cassazione avverso l'ordinanza del Tribunale del riesame di Palermo con cui, ritenuti sussistenti i gravi indizi di colpevolezza sulla base di elementi conoscitivi ottenuti mediante l'utilizzo di un captatore informatico, veniva applicata la misura della custodia cautelare in carcere. Anche in tal caso la difesa, così come era avvenuto in occasione della vicenda Musumeci, aveva lamentato la violazione degli artt. 14 e 15 Cost. e dell'art. 8 CEDU, sottolineando che l'autorizzazione a effettuare le intercettazioni aveva indicato come luogo di captazione «quello ove fosse ubicato in quel momento l'apparecchio portatile». In virtù del richiamo al precedente giurisprudenziale, nel ricorso si sosteneva che, essendo l'indicazione del luogo ove deve svolgersi l'attività captativa un criterio fondamentale di legittimità delle operazioni, nel caso di specie andava dichiarata l'inutilizzabilità delle intercettazioni. Peraltro, il giudice *a quo* dubita dell'effettiva correttezza della decisione del 2015, non avendo tenuto conto della peculiare disciplina prevista per le intercettazioni nel caso in cui si procede per delitti di criminalità organizzata, per cui l'intercettazione di comunicazione tra presenti è consentita anche se non vi è motivo di ritenere che nei luoghi indicati dall'art. 614 c.p. si stia svolgendo l'attività criminosa. (art. 13 d.l. 13 maggio 1991, n. 152 conv. con modificazioni in l. 12 luglio 1991).

privata dimora, ovvero ammetterle esclusivamente in relazione ai delitti di criminalità organizzata.

2.1. *SEGUE*: LA RISOLUZIONE DEL CONFLITTO AD OPERA DELLE SEZIONI UNITE

Nell'«assordante silenzio»[75] legislativo, nel 2016 le Sezioni unite affrontano la questione relativa all'impiego del captatore informatico quale strumento di intercettazione ambientale. Con questa decisione la Corte, in considerazione della natura itinerante dei dispositivi adoperati come moderne microspie e del fatto che tali dispositivi accompagnano le persone nei luoghi "più intimi", afferma che il *virus* possa ritenersi legittimo solo con riferimento «ai procedimenti relativi a delitti di criminalità organizzata, anche terroristica, nonché quelli comunque facenti capo ad un'associazione per delinquere»[76].

In rotta di collisione con la pronuncia del 2015[77], la Suprema Corte sostiene che il riferimento al "luogo" oggetto di intercettazione non debba integrare un presupposto

[75] Così F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, in *Jusonline*, 2017, f. 3, p. 359.

[76] Cass., sez. un., 28 aprile 2016, n. 26889, cit. Diversi sono i commenti alla pronuncia in esame. Si vedano, T. ALESCI, *L'intercettazione di comunicazioni o di conversazioni tra presenti con il* Trojan horse *è ammissibile anche nei luoghi di privata dimora per i reati di criminalità organizzata*, in *Proc. pen. giust*., 2016, f. 5, p. 28 ss.; G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore informatico*", in *Guida dir.,* 2016, f. 34/35, p. 76 ss.; A. CAMON, *Cavalli di Troia in Cassazione,* in *Arch. nuova proc. pen*., 2017, f. 1, p. 91; F. CAJANI, *Odissea del captatore informatico,* in *Cass. pen*., 2016, f. 10, p. 4140 ss.; A. CISTERNA, *Spazio ed intercettazioni, una* liaison *tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *Arch. pen*., 2016, f. 2, p. 331 ss.; G. CORASANITI*, Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Dir. informaz. e inf.,* 2016, p. 88 ss.; P. DI STEFANO, *Grande fratello sì, intercettazioni con lo* smartphone *ma solo per la criminalità organizzata,* in *Foro it.,* 2016, f. 2, p. 513 ss.; P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento* penale: *evoluzione giurisprudenziale e prospettive di riforma,* cit., p. 120 ss.; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia*, cit., p. 359 ss.; W. NOCERINO, *Le Sezioni Unite risolvono l'enigma*: *l'utilizzabilità del "captatore informatico" nel processo penale,* cit., p. 3589. Si vedano anche le riflessioni più generali di G. BARROCU, *Il captatore informatico. Un* virus *per tutte le stagioni*, in *Dir. pen. proc*., 2017, f. 3, p. 379 ss.; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in AA. VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 240 ss.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 53 s.; L. GIORDANO, *La disciplina del "captatore informatico"*, cit., p. 252 s.; ID., *L'uso di captatori informatici nelle indagini di criminalità organizzata,* in *Cass. pen*., 2017, f. 5, p. 208 ss.; G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "tra presenti*", in *Dir. pen. cont*., 7 ottobre 2016; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 108 s.; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 934 s. Da ultimo, L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte,* in *Sist. pen*., 2020, f. 4, p. 109 ss.

[77] Cass., sez. VI, 26 maggio 2015, n. 27100, cit.

dell'autorizzazione a procedere[78], risultando indispensabile solo nella misura in cui concorre a individuare la disciplina applicabile al caso concreto.

Più in particolare, l'art. 266, comma 2 c.p.p. delinea due differenti tipologie di intercettazioni, quelli "ambientali", ossia le captazioni di conversazioni e comunicazioni tra presenti, e quelle "ambientali domiciliari", allorquando l'apprensione del flusso comunicativo avviene nei luoghi di privata dimora di cui all'art. 614 c.p. Di qui, l'indicazione del luogo rileva solo in relazione all'eventuale coinvolgimento di un domicilio privato, dal momento che in tale ipotesi l'attività intrusiva è consentita solo a condizione che sussista un fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa.

Con una precisazione. Una simile condizione non è richiesta nel caso in cui si proceda per delitti di criminalità organizzata, anche terroristica, per cui vige la speciale norma derogatrice dettata dall'art. 13 del d.l. 13 maggio 1991, n. 152, convertito in l. 12 luglio 1991, n. 203[79].

Sul presupposto che risulti impossibile prevedere in anticipo i luoghi in cui la captazione avrebbe avuto luogo, i giudici arrivano a sostenere che l'intercettazione "itinerante" determinata dall'inoculazione di un *virus* su un dispositivo elettronico portatile non possa ritenersi ammissibile per i reati comuni[80]; viceversa, deve considerarsi

---

[78] Come evidenziato dalla Corte, «l'indicazione di uno specifico luogo non risulta inserita né nell'art. 266, comma 2 c.p.p., né nella giurisprudenza della Corte europea dei diritti dell'uomo». Come rilevato dalla giurisprudenza europea, «[...] il contenuto dell'autorizzazione deve identificare chiaramente la specifica persona da sottoporre a sorveglianza oppure l'unico insieme dei luoghi rispetto ai quali viene ordinata l'intercettazione». Così Corte EDU, 18 maggio 2010, *Kennedy c. Regno Unito,* n. 26839/05, in *www.osservatoriocedu.eu*. Nello stesso senso, Corte EDU, 30 aprile 2013, *Cariello c. Italia,* n. 14064/07, in *www.giustizia.it;* 11 giugno 2016, *D'Auria e Balsamo c. Italia*, n. 11625/07, *ivi*. Ma già CEDU 16 ottobre 2007, *Graviano c. Italia,* n. 24320/03, *ivi*. Si possono indicare, a questo punto, indicare due punti fermi: da una parte, il decreto autorizzativo delle intercettazioni di comunicazioni tra presenti deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire solo quando si tratta di luoghi di privata dimora, con la limitazione che, in detti luoghi, tale intercettazioni possono essere effettuate «soltanto se vi è fondato motivo di ritenere che in essi si stia svolgendo l'attività criminosa»; dall'altra, per le intercettazioni di comunicazioni tra presenti da espletare in luoghi diversi da quelli indicati dall'art. 614 c.p. deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta. Così Corte EDU, 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 66610/10, in *www.archiviopenale.it*. In tema, E. BASILICO-S. MARIANI, *Monitoraggio Corte Edu dicembre 2015*, a cura di G. Ubertis- F. Viganò, 15 marzo 2016, in *www.penalecontemporaneo.it.* Si veda, inoltre, Corte EDU, 23 febbraio 2016, Capriotti c. Italia, n. 28819/12, in *www.archiviopenale.it*. Cfr. A. BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*, cit., p. 2278 ss.

[79] Sulla disciplina "differenziata" prevista per i reati "gravi" di criminalità organizzata e terrorismo, si rinvia a nt. 66.

[80] Secondo una diversa lettura della sentenza, l'intercettazione di comunicazioni tra presenti tramite utilizzo del *trojan*, sarebbe stata considerata ammissibile dalle Sezioni unite anche in procedimenti non relativi a criminalità organizzata, in luoghi diversi da quelli *ex* art. 614 c.p., purché preventivamente indicati nella richiesta di intercettazione. In questo senso, F. CAJANI, *Odissea del captatore informatico*, cit., p. 4140. Una simile interpretazione sembra essere suggerita anche da una pronuncia successiva. Cfr. Cass., sez. V, 20 ottobre 2017, n. 48370, in *Giur. it.,* 2017, n. 11, p. 2498, per cui «[S]sono legittime le intercettazioni di comunicazioni informatiche o telematiche, di cui all'art. 266 *bis* c.p.p., effettuate mediante l'istallazione di un captatore informatico (c.d. "*trojan horse*") all'interno di un computer collocato in un luogo di privata dimora». Nel testo della sentenza si legge che con la pronuncia delle Sezioni unite Scurato l'impiego dei captatori informatici non è

legittima nel caso in cui si proceda per delitti di criminalità organizzata, anche terroristica, per cui le captazioni ambientali domiciliari sono sempre consentite.

Una volta circoscritta la "funzionalità" del captatore e individuata la tipologia di reati per cui l'intercettazione a mezzo *Trojan* è legittima, la Corte procede a determinare la corretta nozione di "criminalità organizzata"[81]. Disattendendo quanto auspicato dalla Procura generale, i giudici ne prediligono un'interpretazione assai ampia, ricomprendendo nella stessa «non solo i reati indicati nell'art. 51, commi 3 *bis* e 3 *quater* c.p.p., ma anche quelli comunque facenti capo ad un'associazione per delinquere, *ex* art. 416 c.p., correlata alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato»[82].

Certamente, l'approdo ermeneutico dei giudici di legittimità è determinato dalla ricerca di un punto di equilibrio tra l'esigenza di efficientamento delle indagini e la tutela dei diritti inviolabili. Così, l'uso di nuovi strumenti tecnici, idonei a consentire il «recupero dell'efficacia perduta»[83] delle investigazioni, da una parte, viene limitato sotto il profilo funzionale, per non pregiudicare eccessivamente le prerogative individuali[84]; dall'altra se ne estende l'impiego ad una moltitudine di reati "speciali", in ragione delle maggiori difficoltà nel procedere con le metodologie tradizionali.

Eppure, la pronuncia delle Sezioni Unite ha avuto un'ampia risonanza: da una parte, l'eco di una simile impostazione inebria la giurisprudenza successiva che tende a conformarsi ai principi di diritto enucleati nel 2016[85]; dall'altra suscita reazioni molto

---

stato escluso né per le intercettazioni tra presenti nei luoghi di privata dimora ove si stia svolgendo l'attività criminosa, né per le ulteriori forme di intercettazione. Sulla pronuncia in esame, S. ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante* screen shot, in *Dir. pen. proc*., 2018, f. 8, p. 1065 ss.; C. PARODI, *Intercettazioni telematiche e il captatore informatico: quali limiti?,* in *www.ilpenalista.it*, 6 novembre 2011; A. TESTAGUZZZA, *Ancora in tema di captatore: le intercettazioni informatiche e telematiche. La Cassazione chiede il* bis, in *Giur. it.,* 2017, f. 11, p. 2499 ss. Conforterebbe questa tesi l'orientamento poi seguito dal legislatore, su cui v. *infra* § 5. *Contra* la giurisprudenza più recente. Secondo Cass., sez. I, 25 giugno 2019, n. 50972, in *C.E.D. Cass*., n. 277862, «[N]nei procedimenti relativi a reati diversi da quelli di criminalità organizzata (nella specie, omicidio scaturente da rancori legati a vicende sentimentali), per i quali non sussista fondato motivo di ritenere che nei luoghi indicati dall'art. 614 c.p., si stia svolgendo attività criminosa, sono inutilizzabili i risultati di intercettazioni di comunicazioni tra presenti disposte - prima dell'entrata in vigore delle modifiche apportate all'art. 266c.p.p. dal d.lgs. 29 dicembre 2017, n. 216 - mediante l'installazione di un captatore informatico in un dispositivo elettronico, pur quando il provvedimento autorizzativo preveda che l'esecuzione delle operazioni possa avvenire solo in luoghi diversi da quelli di privata dimora». Nello stesso senso sez. VI, 13 giugno 2017, n. 36874, in *Dir. pen. cont.*, 27 settembre 2017.

[81] Per un approfondimento sul tema *de qua*, si rinvia a Cap. 3, § 3.

[82] Critica una simile scelta, in ragione dell'ampiezza della nozione di "criminalità organizzata", Così M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* cit., p. 36 s.

[83] L'espressione appartiene a E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in *La parola alla difesa*, 2016, f. 9, p. 161.

[84] In questo senso, A. TESTAGUZZA, voce Virus *informatico*, cit., p. 935.

[85] Cass., sez. VI, 3 maggio 2016, n. 27404, in *Quot. giur*., 2016, con cui la Cassazione ha ritenuto infondato tale ricorso sulla base del fatto che l'utilizzo del *virus* informatico «implicava necessariamente una captazione dinamica, non correlata a specifici luoghi, ma dipendente dalla concreta collocazione del dispositivo» e, inoltre, «il tenore dell'autorizzazione non implicava indeterminatezza dello strumento, ma semplicemente postulava una determinata tecnica di

diverse in dottrina, seppure accomunate dall'auspicio di un tempestivo intervento legislativo. Vi è chi ha posto in luce la limitatezza d'interpretazione della Suprema Corte che si è cimentata solo sul tema delle intercettazioni tra presenti nel domicilio, senza considerare le altre potenzialità invasive del captatore informatico[86]; chi, in chiave assai critica, ritiene che la Corte di Cassazione abbia aperto, anche se solo parzialmente, ad un «utilizzo disinibito dell'intrusore informatico»[87], sostenendo che «l'idea di un controllo quasi totale della persona da parte di sistemi privi di specifica disciplina e quasi del tutto incontrollabili sul piano tecnico possa apparire oltre che paradossale, non collimante con le stesse garanzie offerte dall'art. 15 Cost., […] facendo della bulimia investigativa la regola»[88].

Anche il mondo accademico, all'indomani del deposito delle motivazioni delle Sezioni Unite, prende posizione con un appello al legislatore, sollecitato a intervenire delineando specifiche disposizioni frutto di un adeguato bilanciamento dei princìpi costituzionali (artt. 14, 15 e 16 Cost.) e convenzionali (art. 8 CEDU) coinvolti[89].

---

captazione», affermando conclusivamente che «le operazioni sono state autorizzate in relazione ad una determinata metodica e che in concreto avevano riguardato un dispositivo determinabile». Riprendono i principi enunciati dalle Sezioni Unite "Scurato", sez. VI, 3 maggio 2016, n. 26054, non massimata; sez. maggio 2016, n. 26055, non massimata; sez. VI, 3 maggio 2016, n. 26058, non massimata; sez. VI, 13 giugno 2017, n. 36874, cit., con nota di L. GIORDANO, *la prima applicazione della sentenza "Scurato" nella giurisprudenza di legittimità*; sez. VI, 28 febbraio 2017, n. 15573, in *C.E.D. Cass*., n. 269950; sez. V, 20 ottobre 2017, n. 48370, cit.; sez. I, 28 giugno 2017, n. 29169, in *Cass. pen*., 2018, f. 4, p. 343 ss., con nota di L. GIORDANO, *Le prime applicazioni della sentenza "Scurato" nella giurisprudenza di legittimità. La legge n. 103 del 2017*; sez. VI, 8 marzo 2018, n. 45468, in *Dir. pen. proc.*, 2019, f. 5, p. 697, con nota di C.R. BLEFARI, *Le intercettazioni nei confronti di soggetti non indagati*. Da ultimo, sez. I, 25 giugno 2019, n. 50972, cit. Sul punto anche diverse pronunce di merito. Cfr. Tribunale di Modena, 28 settembre 2016, in *www.giurisprudenzapenale.com*; Tribunale di Milano, 13 maggio 2016, in www.dejure.it; Tribunale di Palermo, sez. riesame, 11 gennaio 2016, in *www.penalecontemporaneo.it*; Tribunale di Roma, sez. I, 10 agosto 2015, in *www.dejure*.it. Per una disamina della giurisprudenza *post* Scurato, M.T. ABBAGNALE, *In tema di captatore informatico*, cit., p. 23; L. GIORDANO, *L'uso di captatori informatici nelle indagini di criminalità organizzata,* cit., p. 213 s.; ID, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte,* cit., p. 114 ss.

[86] Così A. SCALFATI, *Un ciclo giudiziario "travolgente*", in *Proc. pen. giust.,* 2016, f. 4, p. 114.

[87] A. TESTAGUZZA, Exitus acta probat. "Trojan" *di Stato: la composizione di un conflitto*, cit.

[88] Si esprime in tal modo L. FILIPPI, L*'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, cit., p. 352.

[89] Cfr. AA.VV., *Necessaria una disciplina legislativa in materia di captatori informatici (c.d.* "trojan"): *un appello al legislatore da parte di numerosi docenti di diritto italiani*, in *Dir. pen. cont.,* 7 ottobre 2016. Una diversa opinione (R. ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen.* online, 25 luglio 2016), invece, ha invitato a distinguere l'uso della moderna tecnologia informatica per effettuare intercettazioni tra presenti – che trova nelle disposizioni dapprima citate la fonte "base normativa" – dal suo impiego per svolgere altre attività di ricerca della prova, come perquisire a distanza gli archivi di computer, *tablet, smartphone* (Cfr., Cap. II). Sotto quest'ultimo aspetto è stato affermato che l'impiego del nuovo strumento esulerebbe dal raggio d'azione degli art. 14 e 15 Cost. e, dunque, non basterebbe l'introduzione di una specifica disciplina normativa, ma sarebbe necessario l'affermazione di un nuovo diritto fondamentale all'uso libero e riservato delle tecnologie informatiche.

Non manca chi assume toni più cauti, valorizzando il pregio del percorso argomentativo e della struttura logica della sentenza[90] e sottolineando come la Suprema Corte, avvertito il pericolo per la riservatezza dell'indagato e dei terzi con lui comunicanti, abbia cercato un compromesso tra libertà individuale e sicurezza collettiva[91].

3. DA *QUERELLE* GIURISPRUDENZIALE A PRIORITÀ PARLAMENTARE. LE PROPOSTE DI LEGGE PER UNA DIGNITÀ NORMATIVA AI NUOVI STRUMENTI INVESTIGATIVI

Nel giro di pochi mesi dalla pronuncia "Scurato", la *quaestio* relativa all'utilizzabilità del *virus* informatico nel processo penale, da argomento "di nicchia" materializzatosi nelle aule di giustizie per iniziativa di alcune procure, diventa il fulcro del dibattito politico e parlamentare.

L'esigenza di un'esaustiva disciplina, al riguardo, si manifesta ripetutamente, concretizzandosi in diverse iniziative legislative finalizzate all'introduzione di una normativa *ad hoc* atta a disciplinare l'impiego dei captatori informatici alla luce dei canoni di proporzionalità e di necessità dell'ingerenza pubblica nella vita privata[92].

Nonostante il percorso giurisprudenziale sia stato più o meno lineare nell'attribuire allo strumento la veste di una «cimice informatica»[93] al solo fine di captare comunicazioni o conversazioni tra presenti, i disegni di legge – almeno nel primo periodo – propendono per un diverso inquadramento giuridico all'attività *de qua*, collocandola nel *genus* delle intercettazioni telematiche.

Per un verso, in sede di conversione del d.l. 18 febbraio 2015, n. 43[94], viene proposto un emendamento per la modifica dell'art. 266 *bis* c.p.p., al fine di inserire una previsione per cui l'intercettazione dei flussi di comunicazioni relative a sistemi informatici o

---

[90] W. NOCERINO, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale,* cit., p. 3580.

[91] In questo senso P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 122, per cui «la vicenda in esame è uno specchio dei tempi in cui viviamo […] in certi momenti storici, si determina una trasformazione del processo da strumento di garanzia a mezzo di contrasto della criminalità con una flessione delle garanzie processuali e individuali».

[92] Per una puntuale disamina delle summenzionate proposte legislative, D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 562; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 130; L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, cit., p. 190 s.; A. TESTAGUZZA, voce Virus *informatico*, cit., p. 937; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 115; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., 49 s.: E. TURCO, *La ricerca della prova ad alta efficacia intrusiva*, in AA. VV., *La riforma della giustizia penale*, a cura di A. Scalfati, Giappichelli, 2017, p. 307 ss.

[93] Così definita da D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 571.

[94] D.l. 18 febbraio 2015, n. 7, convertito, con modificazioni, nella l. 17 aprile 2015, n. 43, recante "*Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale [...]*", in *Gazz. uff*., 20 aprile 2015, n. 91. Per una disamina approfondita degli innesti normativi della novella, esaustivamente, in AA. VV., *Il nuovo "pacchetto" antiterrorismo*, a cura di R.E. Kostoris–F. Viganò, Giappichelli, 2015, p. 4 ss.

telematici avrebbe potuto essere effettuata «anche attraverso l'impiego di strumenti o programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico»[95].

Tale disposizione viene, però, stralciata in ragione delle implicazioni che dallo stesso sarebbero derivate[96]. Troppo pericoloso, infatti, sarebbe stato l'innesto: il succitato articolo, nel delineare l'ambito applicativo delle intercettazioni informatiche o telematiche, richiama il criterio qualitativo di cui all'art. 266, comma 1 c.p.p., che inerisce a tutta una serie di fattispecie delittuose assai diversificate tra loro – ma, sul piano edittale, di entità assai inferiore – rispetto ai reati di terrorismo oggetto della legge[97].

Per altro verso, l'eco suscitato dall'attentato al Bataclan, in Francia, rafforza la consapevolezza dell'indispensabilità del ricorso ai nuovi strumenti di indagine. A distanza di pochi mesi dal tragico evento, viene depositato alla Camera dei Deputati il disegno di legge d'iniziativa della deputata Greco, del 2 dicembre 2015, concernente la modifica dell'art. 266 *bis* c.p.p. in materia di intercettazioni informatiche e telematiche[98].

Nella Relazione di accompagnamento di osserva che l'innalzamento della minaccia terroristica «costituisce una gravissima insidia per la sicurezza interna e internazionale», sottolineandosi che, per adeguare la risposta investigativa a tali minacce, occorre consentire l'uso «di programmi informatici che permettano l'accesso da remoto ai dati presenti in un sistema informatico al fine di contrastare preventivamente i reati di terrorismo commessi mediante l'uso di tecnologie informatiche o telematiche». Ma anche un simile tentativo di regolamentare l'ingresso dei nuovi strumenti di indagine non sortisce l'effetto sperato.

Dopo una prima ondata riformista tutta incentrata alla modifica dell'art. 266 *bis* c.p.p., si assiste a nuovi tentativi progressisti tesi ad operare modifiche assai più ampie e incisive, che vanno dalla riformulazione di tutte le norme disciplinanti i singoli mezzi di ricerca della prova (artt. 244, 247 252, 266 ss. c.p.p.), con il precipuo intento di adeguare l'obsoleto codice di rito alla nuova realtà tecnologica, fino alla predisposizione di una normativa *ad hoc,* interamente dedicata alle acquisizioni da remoto.

Più in particolare, viene depositata una nuova proposta di legge d'iniziativa dei deputati Quintarelli e Catalano[99], nella quale l'impiego del "captatore legale" viene

---

[95] Si vedano, sul punto, i subemendamenti del Governo presentati in data 19 marzo 2015 – Bollettino delle Giunte e delle Commissioni Parlamentari – Commissioni Riunite (II e IV) – All. 1.

[96] La modifica non trova accoglimento nemmeno dopo un emendamento teso a limitare l'orbita applicativa del *virus* ai soli delitti commessi con finalità di terrorismo (artt. 270 *bis*, 270 *ter*, 270 *quater* e 270 *quinquies* c.p. commessi con finalità di terrorismo di cui all'art. 270 *sexies* c.p.). Cfr. Proposta di modifica n. 2206 del d.d.l. 2895, in riferimento all'art. 2, presentato il 26 marzo del 2015 in Assemblea alla Camera dall'on. Quintarelli.

[97] In questo senso D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 570.

[98] Cfr. Proposta di legge C. 3470, 2 dicembre 2015, recante "*Modifica all'articolo 266*-bis *del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche*", presentata il 2 dicembre 2015.

[99] Proposta di legge C. 3762, recante "*Modifiche al codice di procedura penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, in materia di investigazioni e sequestri relativi a dati e comunicazioni contenuti in sistemi informatici o telematici*", presentata il 20 aprile 2016.

previsto nell'ambito di tutti i mezzi di ricerca della prova, nel rispetto delle garanzie individuali[100].

Da ultimo, prima che con la l. 23 giugno 2017, n. 103 si intervenisse a disciplinare l'istituto *de quo*, rinviando ad una successiva delega gli aspetti salienti della normativa[101], il 31 gennaio 2017 viene presentata alla Camera una nuova proposta di legge[102], assai ampia e articolata, contenente una disciplina dettagliata di tre diversi attività investigative esperibili mediante il *virus* informatico: l'osservazione dei dispostivi e l'acquisizione da remoto dei dati contenuti in un sistema informatico o telematico diversi da quelli relativi al traffico telefonico o telematico, da realizzarsi attraverso l'introduzione di un inedito mezzo di ricerca della prova (art. 254 *ter* c.p.p.)[103]; le intercettazioni di conversazioni e

[100] Più in particolare, la proposta mira a: disciplinare l'istituto della perquisizione a distanza nei soli casi in cui si fosse proceduto per i reati di cui agli artt. 51, commi 3 *bis*, 3 *quater* e 3 *quinquies* c.p.p., nonché all'art. 407, comma 2 c.p.p. e ai delitti dei pubblici ufficiali contro la pubblica amministrazione (art. 1); normare le tecniche di sequestro da remoto dei dati "diversi da quelli relativi al traffico telefonico o telematico", limitatamente ai reati sopra indicati (art. 2); modificare l'art. 266 *bis* c.p.p., al fine di disciplinare l'uso dei captatori informatici per compiere l'intercettazione dei flussi di dati e per la localizzazione geografica del dispositivo (art. 3); prevedere il carattere sussidiario e residuale dell'impiego dello strumento investigativo (art. 4); modificare l'art. 268 c.p.p. ai fini della conservazione dei dati informatici acquisiti con le modalità tali da assicurare l'integrità e l'immodificabilità di quanto raccolto e la loro conformità all'originale (art. 5); inserire una nuova norma (art. 89 *bis* al d.lgs. 271/1989), con il fine di indicare i contenuti del decreto ministeriale sulle caratteristiche tecniche dei programmi informatici (art. 6); modifica dell'art. 226 disp. att. c.p.p. per consentire l'adeguamento della disciplina delle intercettazioni preventive al nuovo strumento di captazione (art. 7).

[101] Sul punto, v. § 4 e 5.

[102] Proposta di legge n. 4260, recante "*Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi*", ad iniziativa degli on. Quintarelli, Basso, Stella Bianchi, Bombassei, Bruno Bossio, Carrozza, Catalano, Coppola, Dallai, Dambruoso, Fiano, Galgano, Librandi, Longo, Marzano, Mazziotti Di Celso, Menorello, Monchiero, Mucci, Nesi, Palladino, Palmieri, Vargiu, presentata il 31 gennaio 2017 e assegnata alla II Commissione Giustizia *in sede* Referente l'8 marzo 2017. Per un'ampia disamina dell'articolato, F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 503 ss.; A. TESTAGUZZA, voce Virus *informatico*, cit., p. 938.

[103] In particolare, l'art. 1 della Proposta di legge consentiva, di procedere all'osservazione delle attività realizzate con i dispositivi e all'acquisizione da remoto dei dati contenuti in un sistema informatico o telematico, diversi da quelli relativi al traffico. In ragione della pervasività del mezzo, il suo esperimento si riteneva dovesse essere subordinato a diverse condizioni. Prima di tutto, si prevedeva che l'utilizzo fosse possibile solo qualora si proceda per i reati di criminalità organizzata, limitatamente a quelle fattispecie che risultavano talmente pervasive per cui non era possibile distinguere un ambito di attività o di vita personale estraneo all'associazione criminale, come sono quelli relativi al terrorismo e alle associazioni mafiose. Inoltre, si prevedeva che il pubblico Ministero non potesse disporre autonomamente la captazione, ma dovesse richiedere l'autorizzazione al giudice per le indagini preliminari. Il giudice avrebbe potuto concedere tale autorizzazione solo qualora vi siano stati gravi indizi di reato e qualora l'osservazione e l'acquisizione da remoto fossero veramente utili e assolutamente indispensabili per la prosecuzione delle indagini. Attraverso il richiamo agli articoli 266 *bis* 1 *quater* e 1 *quinquies* ss. c.p.p., si prevede l'applicazione al nuovo mezzo di ricerca della prova di numerose norme che già disciplinano le intercettazioni informatiche e telematiche, in quanto compatibili (in particolare, in materia di durata ed esecuzione delle operazioni, ecc.). Tuttavia, a differenza che nelle intercettazioni informatiche, l'esecuzione materiale delle operazioni si penso di demandarla alla sola polizia giudiziaria, escludendo la possibilità di avvalersi di ausiliari esterni.

comunicazioni, anche tra presenti, attraverso una modifica degli artt. 266 ss. c.p.p.[104]; l'acquisizione della posizione geografica della persona sottoposta alle indagini mediante l'inserimento di un nuovo art. 226 *ter* c.p.p.[105].

Non solo. Alla regolamentazione in senso specifico delle attività investigative eseguibili mediante captatore, da utilizzare solo quale *extrema ratio*[106], si affianca la limitazione delle tipologie delittuose per cui lo strumento può trovare regolare impiego, ossia in procedimenti per reati di criminalità organizzata di stampo mafioso o con finalità di terrorismo[107]. Senza considerare, poi, le decisive innovazioni sul piano tecnico, tese, da un a parte, a garantire il rispetto delle garanzie di cui agli artt. 267, 268 e 269 c.p.p.[108], dall'altra, a predisporre i requisiti specifici affinchè tali programmi possano essere definiti "legali"[109].

---

[104] L'art. 2 della Proposta di legge interviene sull'art. 266 *bis* c.p.p., disciplinando espressamente, con quattro nuovi commi, l'uso dei captatori al fine di intercettare comunicazioni o conversazioni, anche tra presenti. Tale modalità di intercettazione era consentita solo in riferimento ai delitti indicati nel nuovo articolo 254 *ter* comma 1 c.p.p.

[105] L'art. 3 della proposta, introduttivo di un nuovo art. 266 *ter* c.p.p., prevedeva anche la possibilità di attivare, per il tramite del captatore, le funzioni di acquisizione della posizione geografica del dispositivo.

[106] L'art. 4, oltre ad alcune modifiche di coordinamento, prevedeva che le operazioni di cui all'art. 266 *bis*, commi 1 *bis* e 1 *ter* c.p.p. potessero essere autorizzate solo quando ogni altro mezzo di ricerca della prova risultasse inadeguato. Vista l'estrema invasività dello strumento, si cercò di optare per limitarne l'uso, come *extrema ratio.* Sia la richiesta del PM, sia il provvedimento del giudice, avrebbero dovuto quindi essere motivate sul punto.

[107] Come si legge nella Relazione di accompagnamento alla proposta, «[È]è evidente che vi sono altre tipologie di reati molto gravi, che destano ribrezzo e sdegno sociale, per contrastare i quali l'utilizzo del captatore può offrire grandi possibilità, primo tra tutti la pedopornografia». Tuttavia si decise di arrivare e attestarsi su un punto di equilibrio con i diritti costituzionali. Punto di assai difficile individuazione ma necessario. la definizione del perimetro di applicabilità fu un quindi un tema estremamente delicato. In questa proposta, oltre a definire con cura le garanzie delle parti e del procedimento, i proponenti avevano ritenuto opportuno limitare il perimetro dell'utilizzabilità, ai soli reati che attentano alla integrità dello Stato e avevano demandato ad una approfondita riflessione nel Parlamento, sede del processo democratico, il perimetro di utilizzabilità più appropriato.

[108] L'art. 5 introduceva l'art 268 *bis* c.p.p., con il quale si prevedevano ulteriori garanzie per lo svolgimento mediante programmi e strumenti informatici delle attività di cui agli artt. 268 *bis* e 268 *ter* c.p.p. Si è ritenuto che gli strumenti e i programmi utilizzati devono assicurare che i dati presenti sul dispositivo non venissero alterati o modificati e che i dati acquisiti fossero conformi a quelli originali presenti sul dispositivo medesimo. Ugualmente, anche per la conservazione dei dati (una copia dei quali doveva essere conservata negli uffici o negli impianti della Procura) si pensò di garantire l'integrità, la genuinità e l'immodificabilità. Si prevedeva poi che il giudice, nel proprio decreto, fosse in grado di individuare i singoli dispositivi oggetto di captazione. In tal modo, si voleva evitare che il decreto diventi un'autorizzazione "in bianco" al p.m., tale da consentirgli un controllo sproporzionato sulla vita del soggetto, operato attraverso la captazione di un numero potenzialmente indeterminato di dispositivi. Sempre nell'ottica di garantire la genuinità dell'operazione di captazione, il comma 5 stabiliva penetranti obblighi di documentazione della stessa, anche in relazione ai soggetti che vi prendono parte e ai programmi che vengono impiegati. Al termine delle operazioni le norme ipotizzate prevedevano che il captatore dovesse essere rimosso dal dispositivo e di tale operazione doveva essere redatto un verbale di polizia giudiziaria; in caso di impossibilità di rimozione, devono essere fornite all'utente le istruzioni per provvedervi autonomamente. Il comma 8 prevedeva poi che i captatori possedessero i requisiti da stabilirsi con apposito regolamento del Ministro della Giustizia, emanato di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali.

[109] L'art. 6 aggiungeva un nuovo articolo 89 *bis* al d.lgs n. 271/1989 (norme di attuazione, di coordinamento e transitorie del codice di procedura penale), indicando i contenuti necessari del

L'articolato non è mai andato in discussione in Commissione anche a causa della fine della legislatura ma, nonostante le molte critiche ricevute, è considerato un buon testo dal quale ripartire se e quando i tempi saranno maturi. In particolare, si è detto che «[Q]questa previsione appare la più opportuna, riuscendo a coniugare le esigenze di difesa sociale, legate alla necessità investigativa di intercettare flussi di comunicazioni altrimenti non intercettabili, perché criptate, come ormai quasi tutti le forme di comunicazione di natura telematica, e le istanze difensive di "monitoraggio" della correttezza dell'operato della polizia giudiziaria»[110].

4. IL CAPTATORE INFORMATICO NELLA *MAXI* RIFORMA "ORLANDO". CRITERI DIRETTIVI

Con un'anomala inversione di tendenza[111], la regolamentazione dell'impiego del captatore informatico nel processo penale è posposta all'interpretazione

futuro decreto sui captatori previsto dal citato art. 5, comma 8, prescrivendo l'aggiornamento almeno ogni tre anni. In particolare, si preciso che i requisiti tecnici individuati dal decreto dovevano assicurare che l'installazione e l'attività dei captatori non alterasse i dati acquisiti, né le restanti funzioni del dispositivo. Sempre al fine di fornire un valido contrappeso all'utilizzo di questo potente e invasivo strumento investigativo, si era tentato di inserire dei criteri direttivi ai quali i Ministeri competenti avrebbero dovuto conformarsi nell'emanazione del decreto, così da garantire: l'istituzione di un sistema di omologazione dei captatori, affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM); il diritto per la difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dalla lo installazione fino alla loro rimozione, e di verificare tecnicamente che i captatori in uso siano certificati, fino a consentire l'ispezione del codice sorgente - previamente depositato presso un ente da determinarsi - e gli accertamenti tecnici informatici volti a verificare l'assenza di manipolazioni; la possibilità per la difesa, con tutte le garanzie del caso e gli obblighi di riservatezza e segreto, di verificare gratuitamente la presenza del captatore utilizzato in un registro nazionale dei captatori, gestito dall'ente di omologazione; la registrazione di tutte le operazioni svolte dal captatore, dalla sua installazione fino alla sua rimozione, poi messe integralmente a disposizione delle parti come allegato del fascicolo; che il captatore non determini un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene utilizzato; la disinstallazione dei programmi al termine dell'uso autorizzato, anche fornendo all'utente le informazioni necessarie a provvedervi autonomamente in alcuni casi; l'obbligo per i produttori di fornire pubblicamente e gratuitamente gli strumenti *software* necessari per l'analisi dell'allegato al fascicolo contenente la registrazione delle operazioni; la possibilità per le parti di richiedere ed eseguire in modo indipendente la verifica del processo di omologazione. Solo per dovere di completezza, si enunciano le ulteriori modifiche previste. L'art. 7 modificava invece il preesistente art. 226 disp att. c.p.p., al fine di adeguarne il contenuto all'introduzione dell'art. 254 *ter* e alle modifiche all'art. 266 *bis* c.p.p. L'art. 8 prescriveva che gli articoli da 1 a 7 della nuova normativa trovassero applicazione alle attività di indagine avviate o proseguite dopo 90 giorni dalla pubblicazione in Gazzetta Ufficiale del decreto ministeriale sugli strumenti di osservazione e acquisizione da remoto. L'art. 9 prevedeva un aumento delle pene qualora strumenti di osservazione e acquisizione da remoto fossero stati usati per scopi criminali cagionando danni alla sicurezza nazionale e alle infrastrutture critiche del Paese o qualora l'intrusione informatica fosse avvenuta al fine di trattare illecitamente dati personali sensibili o giudiziari, o comunque se a seguito dell'intrusione informatica tali dati fossero stati diffusi illecitamente.

[110] Così D. CURTOTTI-W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 563.

[111] Come sottolinea M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, Editoriale Scientifica, 2019, p. 15, «[P]profilo dimostrativo della "caduta" che la storia contemporanea

giurisprudenziale: solo dopo quasi un anno dalla fatidica pronuncia del Supremo Collegio[112], il Parlamento, ravvisata l'inquietudine della comunità giuridica[113], sveste i panni di organo supremo decontestualizzato dalla realtà esistente e decide di mettere un punto fermo alla *quaestio*, delineando i confini e i limiti entro cui consentire le intercettazioni a mezzo *Trojan* nonché disciplinando le modalità di esecuzione delle operazioni predette.

Il *leitmotiv* che permea la *ratio* riformatrice risiede nella tutela della riservatezza dei soggetti solo occasionalmente coinvolti dallo strumento captativo e, come tale, almeno secondo la relazione di accomunamento del decreto, l'intera novella dovrebbe essere interpretata alla luce della predetta garanzia a tutela della *privacy*[114].

Tuttavia, il delegante sembra più concentrato a "normativizzare" – modificandoli *in peius* – i *dicta* giurisprudenziali[115], le direttive del CSM nonché le Circolari delle Procure maggiormente influenti[116] - in modo da rendere "appetibile" la riforma soprattutto agli occhi della magistratura -, che ad introdurre previsioni atte a cercare un equilibrio tra l'invasività propria dello strumento e le prerogative individuali.

---

manifesta […] è fornito dal dominio della giurisprudenza sulla procedura e dalla egemonia delle prassi sul processo; situazione che apre al giurista nuovi orizzonti rispetto alla legge, avendo essa perso la natura di "opzione regale" per diventare "prodotto imperfetto"».

[112] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[113] Compendiata nell'appello dei Professori ordinari di diritto processuale penale. Cfr. Cfr. AA.VV., *Necessaria una disciplina legislativa in materia di captatori informatici (c.d.* "trojan"): *un appello al legislatore da parte di numerosi docenti di diritto italiani*, cit.

[114] Come precisato, «[D]dette disposizioni perseguono lo scopo di escludere, in tempi ragionevolmente certi e prossimi alla conclusione delle indagini, ogni riferimento a persone solo occasionalmente coinvolte dall'attività di ascolto e di espungere il materiale documentale, ivi compreso quello registrato, non rilevante a fini di giustizia, nella prospettiva di impedire l'indebita divulgazione di fatti e riferimento a persone estranee alla vicenda oggetto dell'attività investigativa che ha giustificato il ricorso a tale incisivo mezzo di ricerca della prova». Così C.D.M., *D.lgs. – Disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione dell'art. 1, legge 23 giugno 2017, n. 103 – Relazione*, in *www.giurisprudenzapenale.it*.

[115] Sul punto, M. GIALUZ-A. CABIALE-J. DELLA TORRE, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *www.penalecontemporaneo.it*, 20 giugno 2017. Con il riferimento esclusivo alle Sezioni Unite Scurato si sono avverati i timori di parte della dottrina sul tema generale delle indagini informatiche. A causa della tecnica di redazione legislativa imperfetta, invero, si andrebbe incontro a un duplice rischio: «da un lato, quello di legiferare in base ad una concezione di fondo tipica del mondo della rete che tende a prediligere un approccio intuitivo ed emotivo ad uno analitico sistematico. Dall'altro, il rischio che la molteplicità dei problemi che emergono nella prassi applicativa porti il legislatore a risolvere i problemi concreti con un pragmatismo disancorato dai principi», con la conseguenza di «sospingersi nella direzione di un modo di operare caratterizzato dalla precarietà e dalla destrutturazione». Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 47.

[116] *Ex multis*, Procura della Repubblica presso il Tribunale di Napoli, Direttiva n. 1, 2016, in *www.questionegiustizia.it*; Procura della Repubblica presso il Tribunale di Torino, Circolare n. 513/16, 15 febbraio 2016, *ivi*; Procura della Repubblica presso il Tribunale di Roma, Circolare n. 3389/15, 26 novembre 2015, *ivi*. Per una panoramica, A. CAMON, *Intercettazioni e fughe di notizie: dal sistema delle circolari alla riforma Orlando*, in *Arch. pen.,* 2017, f. 2, p. 1 ss.; G. CASCINI, *Intercettazioni e* privacy: *dalle circolari delle Procure di Roma, Torino e Napoli soluzioni utili per il legislatore*, in *Quest. giust.,* 19 aprile 2016; P. TONINI, *Le intercettazioni delle procure della repubblica*, in *Dir. pen. proc*., 2017, f. 6, p. 705 ss.

Prima di analizzare nel dettaglio i criteri individuati, appare indispensabile soffermarsi sul complesso *iter* legislativo che segue il disegno di legge del Senato che porta alla luce la riforma in senso progressista del processo penale[117].

Nelle more del deposito della motivazione delle Sezioni Unite, in Parlamento si comincia ad assistere ad un repentino e confuso movimento di "infiltrazione" di proposte di modifica al disegno di legge n. 2067. In sede di lavori della II Commissione Permanente del Senato, si succedono molteplici emendamenti, tutti a modifica del testo principale di discussione (n. 36.4000) che, tuttavia, inizialmente prevedeva anche l'utilizzo del captatore informatico per l'accertamento dei reati di cui all'art. 416 c.p. Gli emendamenti sono molteplici, quasi una decina, discussi prevalentemente nella seduta del 22 giugno 2016, prima quindi del deposito della motivazione delle Sezioni Unite.

Degno di nota è l'emendamento n. 35.133 (relatori Orellana, Battista) teso da un lato ad eliminare i profili più critici della disciplina come la possibilità che le intrusioni vengano effettate da personale esterno alle forze di polizia, nelle forme dell'art. 348, comma 4 c.p.p., e dall'altro a potenziare le garanzie difensive prevedendo che «al termine delle indagini, sia dato il diritto alla difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dall'installazione fino alla loro rimozione, nonché la possibilità di chiedere al giudice di verificare che il captatore utilizzato rispetti i requisiti previsti dalla normativa vigente». In Senato, il 22 settembre 2016, i relatori presentano l'emendamento depurato dall'ipotesi dell'art. 416 c.p., precisando che: «al fine di consentirne un impiego efficace e allo stesso tempo rispettoso della *privacy* dei cittadini, l'utilizzo di questo strumento rimane sempre consentito, ma con specifica motivazione del giudice, per reati gravi tra cui mafia e terrorismo, ma non per la generica associazione a delinquere (art. 416 c.p.)», richiamando in tal senso la coerenza con la motivazione delle Sezioni Unite.

Da quel momento in poi, l'emendamento segue le sorti legislative del disegno di legge nel quale è ospitato[118].

---

[117] Il Disegno di legge n. 2067 A.S., intitolato "*Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole di processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*", viene approvato dal Senato il 15 marzo 2017. Tale proposta nasce dall'accorpamento in un unico testo di tre progetti di legge già approvati dalla Camera (Atti Camera nn. 2798, 2150 e 1129) e di una pluralità di proposte di legge di iniziativa parlamentare. Esso consta di un unico articolo con ben novantacinque commi, che intervengono sull'intero sistema penale, con norme immediatamente efficaci e diverse deleghe. Per un primo commento sul d.d.l., G. SPANGHER, *DDL n. 2067: sulle proposte di modifica al codice di procedura penale*, in *www.giurisprudenzapenale.com*, 19 marzo 2017.

[118] Il 14 giugno 2017 il testo viene approvato in via definitiva, con il voto di fiducia, dalla Camera dei Deputati (Atto Camera n. 4368), con la modifica del titolo inizialmente previsto in "*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*". Sui lavori preparatori e sulle diverse versioni che si sono succedute, cfr. M. BARGIS, *I ritocchi alle modifiche in tema di impugnazioni nel testo del D.D.L. N. 2798 approvato dalla Camera dei Deputati*, in *Dir. pen. cont*., 19 ottobre 2015; EAD., *Primi rilievi sulle proposte in materia di impugnazioni del recente D.D.L. governativo*, *ivi*, 2015, f. 1, p. 4; S. BELTRANI*, E venne il giorno*!, in *Il Penalista*, 15 giugno 2017; S. LORUSSO, *La giustizia penale tra riforme annunciate e riforme sperate*, in *Proc. pen. giust*., 2017, f. 1, p. 1; G. SPANGHER, *DDL n. 2067: sulle proposte di modifica al codice di procedura penale*, cit.; G. SAMBUCO, *Rafforzamento delle garanzie difensive, durata ragionevole del processo e contrasto alla corruzione,* in *Proc. pen. giust*., 2015, f. 2, p. 17; S. ZIRULIA-L. MATARRESE, *Il Governo presenta alla Camera un articolato pacchetto di riforme del codice penale, del codice di procedura penale e dell'ordinamento penitenziario*, in *Dir. pen. cont*., 15 gennaio 2015.

La definitiva consacrazione del captatore informatico quale nuovo strumento investigativo avviene con la promulgazione della legge 23 giugno 2017, n. 103, che prevede, nell'esercizio della delega di cui al comma 82, l'attuazione di decreti legislativi recanti una nuova forma di intercettazione di conversazioni o comunicazioni tra presenti attraverso l'immissione, in dispositivi elettronici portatili, del captatore informatico[119].

Il comma 84 della l. 103/2017 contempla criteri direttivi (il comma parla, altresì, di "principi", dei quali tuttavia si ritiene non esservi traccia relativamente al tema in esame) al quale il legislatore delegato dovrà attenersi nel disciplinare l'istituto.

I criteri sono molto dettagliati, tanto da far pensare ad una veste normativa pressoché definitiva. Il solo dubbio che investe lo studioso è la sua collocazione nelle norme dedicate alle intercettazioni, ben potendosi prevedere tanto un nuovo comma 2 *bis* dell'art. 266 c.p.p., con un'integrazione degli artt. 268 e 269 c.p.p. per la parte operativa, ovvero un art. 266-*ter* c.p.p., comprensivo dell'intera previsione.

Tali "principi" prevedono che: 1) l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice; 2) la registrazione audio venga avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'art. 348 comma 4 c.p.p., su indicazione della polizia giudiziaria operante che è tenuta a indicare l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'art. 268 c.p.p.; 3) l'attivazione del dispositivo sia sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p. e, fuori da tali casi, nei luoghi di cui all'art. 614 c.p. soltanto qualora *ivi* si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'art. 266 comma 1 c.p.p.; in ogni caso il decreto autorizzativo del giudice deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini; 4) il trasferimento delle registrazioni sia effettuato soltanto verso il *server* della procura così da garantire originalità e integrità

[119] L. 23 giugno 2017, n. 103, cit. Sulla delega per l'adozione di un decreto legislativo che disciplini le intercettazioni mediante captatore informatico si vedano, tra gli altri, P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 329 ss.; D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 570 ss.; L. FILIPPI, *Molte perplessità e poche note positive nella legge delega di riforma delle intercettazioni*, in *www.ilpenalista.it*; ID., *La delega in materia di uso del captatore informativo*, in AA. VV., *La riforma Orlando. Modifiche al Codice penale, al Codice di procedura penale e all'Ordinamento penitenziario*, a cura di G. Spangher, Pacini Giuridica, 2017, p. 151 ss. p. 151 ss.; M. GIALUZ, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazioni della giurisprudenza, riforme attese da tempo e confuse innovazioni,* in *www.penalecontemporaneo.it*, 20 giugno 2017, p. 32 ss.; L. GIORDANO, *La delega per la riforma della disciplina delle intercettazioni (commi 82, 83 e 84, lett. a, b, c, d l. n. 103/ 2017),* in AA. VV., *La riforma della giustizia penale*, a cura di A. Marandola–T. Bene, Giuffrè, 2017, p. 357 ss.; S. LONATI, *I criteri direttivi contenuti nella delega in materia di intercettazioni*, cit., p. 243 ss.; C. PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici",* in *www.magistraturaindipendente.it*; G. SPANGHER, *Aggiornamenti sulla "Riforma Orlando" sul processo penale,* in AA.VV., *Treccani- Il Libro dell'anno 2017*, Treccani, 2017, p. 695 ss.; ID., *La riforma Orlando della giustizia penale: prime riflessioni*, in *Dir. pen. cont.,* 5 ottobre 2016, 98 s.; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 938 s.; E. TURCO, *La ricerca della prova ad alta efficacia intrusiva*, cit., p. 307 ss.; A. ZAMPAGLIONE, *Delega in materia di intercettazioni: un costante bilanciamento di interessi*, in AA. VV., *La riforma Orlando. Modifiche al Codice penale, al Codice di procedura penale e all'Ordinamento penitenziario*, cit., p. 111 ss.

delle registrazioni; al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante; 5) siano utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con decreto ministeriale da emanare entro trenta giorni dalla data di entrata in vigore dei decreti legislativi di cui al presente comma, che tenga costantemente conto dell'evoluzione tecnica al fine di garantire che tali programmi si limitino ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia; 6) fermi restando i poteri del giudice nei casi ordinari, ove ricorrano concreti casi di urgenza, il pubblico ministero possa disporre le intercettazioni di cui alla presente lettera, limitatamente ai delitti di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p., con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendono impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini; 7) i risultati intercettativi così ottenuti possano essere utilizzati a fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e possano essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti di cui all'art. 380 c.p.p.; 8) non possano essere in alcun modo conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede.

Volendo tentare una schematizzazione dei profili maggiormente incisivi della riforma, può dirsi che il legislatore agisce lungo due linee direttrici: da un lato, conformemente a quando indicato dalle Sezioni Unite "Scurato", vengono limitate le potenzialità intrusive del captatore informatico, finendo per rappresentare solo una nuova modalità esecutiva di un vecchio mezzo di ricerca della prova; dall'altro, recependo le obiezioni espresso avverso l'orientamento giurisprudenziale del 2016, la sua sfera operativa viene ancor più limitata e circoscritta, sia con riferimento ai reati intercettabili a mezzo *Trojan* – ovvero nei soli casi in cui si proceda per i reati di criminalità organizzata di tipo mafioso o terroristico di cui agli artt. 51, commi 3 *bis* e 3 *quater* c.p.p.[120] –, sia con riguardo alla sua configurazione quale strumento a carattere eccezionale, cui ricorrere solo quando non è possibile, per la situazione concreta, operare con i mezzi tradizionali di intercettazione.

Pur apparendo encomiabile l'intento di contingentare l'impiego del *virus* ai soli casi e/o reati per cui lo stesso risulta necessario, può ritenersi che il *punctum dolens* della disciplina risieda proprio nell'aver limitato la funzionalità del captatore informatico quale strumento tecnico di intercettazione ambientale, senza preoccuparsi di affrontare tutto il complesso di questioni giuridiche inerenti alle altre attività che il *Trojan*, anche solo in potenza, è in grado di compiere[121].

---

[120] Come anticipato, la Suprema corte aveva ritenuto legittimo l'uso del captatore informatico nei luoghi di privata dimora, prescindendo dallo svolgimento di un'attività criminosa, non solo per i reati di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p. ma anche per quelli definibili di "criminalità organizzata", cioè inquadrabili comunque nelle attività facenti capo ad un'associazione per delinquere *ex* art. 416 c.p., correlata alle operazioni criminose più disparate, con esclusione del mero concorso di persone nel reato.

[121] Di tale "lacuna" nella delega è ben conscio il Governo: «come si ricava dal chiaro tenore della delega e dai sopramenzionati criteri per la sua attuazione, il delegante ha inteso regolamentare uno solo degli usi del captatore informatico, quale modalità specifica di esecuzione delle intercettazioni

Come sostenuto, «il principale aspetto di criticità della legge delega […] non è nella disciplina introdotta ma in ciò che non è stato disciplinato […]. Restano fuori dalle nuove norme gli impieghi che sfruttino qualsiasi altra delle molteplici potenzialità di questi malware, che possono trasformare il dispositivo target in uno strumento di ispezione o perquisizione di "luoghi" o "spazi" digitali, o arrivare ad acquisire tutti i dati sensibili di una persona rastrellando informazioni nei suoi database digitali»[122].

L'assenza di qualsivoglia disciplina relativa all'uso del captatore, oltre la semplice attivazione del microfono, creerebbe una "zona grigia" che gli interpreti sarebbero chiamati ad "illuminare", lasciando «alle procure e alla giurisprudenza il compito di definire modalità, regole, effetti dell'uso del captatore per le attività di ispezione, perquisizione e sequestro e quant'altro è possibile acquisire con lo strumento *de quo*»[123].

In tale contesto, sarebbe stato preferibile un ampliamento della platea dei potenziali impieghi del captatore anche per condurre attività che esulano dal concetto di "intercettazione ambientale" e che la tecnologia permette di compiere[124], in modo da disciplinare – con norme *ad hoc* – le svariate tipologie di investigazioni che, *de facto*, vengono compiute da remoto (quali, ad esempio, perquisizioni, sequestri, acquisizioni di documenti, *files*, dati di localizzazione, accessi sul *cloud*)[125].

---

tra presenti, ed ha ad oggetto esclusivamente dispositivi mobili portatili». Cfr. C.D.M., *D.lgs. – Disposizioni in materia di intercettazione,* cit., p. 9. Vi è poi chi, anche in dottrina, sostiene che «probabilmente i tempi non sono ancora maturi per un'organica disciplina di tutte le attività che possono essere svolti dal captatore informatico». Così F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, cit., p. 357.

[122] P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 346. Nello stesso senso anche L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit. p. 290 s.; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., p. 150, per cui l'impostazione è «minimalista e riduttiva».

[123] G. SPANGHER, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, cit.

[124] Proprio in ragione delle molteplici attività che il captatore informatico è capace di condurre da remoto, si ritiene auspicabile un adeguamento linguistico, in modo da non rendere obsoleta la normativa *neo* introdotta. Come sostenuto, «sarebbe più efficace parlare di "attività di captazione informatica", al fine di prevedere ed estendere a livello normativo le opportune garanzie menzionate proprio dal d.l. n. 161/2019 anche a tutte le altre attività di captazione che la tecnologia rende e renderà possibile nel futuro». Così S. ATERNO, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, *www.senato.it,* p. 3.

[125] In questo senso G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., p. 151. Non si ritiene, tuttavia, condivisibile l'impostazione sostenuta dall'Autore per cui l'applicazione del captatore dovrebbe essere estesa anche alle videoriprese di comportamenti comunicativi e non, a seconda del luogo ove essi vengono a compiersi, domiciliare o meno, dal momento che «pare incomprensibile la ragione per cui, una volta ammesso tale penetrante strumento di indagine, ci si limiti alla sola captazione sonora». Si ritiene, invece, che prevedere la possibilità per il captatore di attivare la videocamera del dispositivo infettato, procurerebbe *ex se* una violazione del principio di diritto enucleato dalla giurisprudenza di legittimità nel 2006 (Cass., sez. un., 28 luglio 2006, n. 26795, cit.), posto a protezione degli artt. 14 e 15 Cost. Né la scelta si può giustificare con l'onere di motivazione rafforzata e l'inutilizzabilità dei dati appresi: non essendo possibile far scattare un divieto *ex ante* di riprendere i comportamenti non comunicativi

5. IL D.LGS. 216/2017. ESEGESI DI UNA DISCIPLINA "FANTASMA"

Il 29 dicembre 2017 viene approvato in via definitiva il d.lgs. n. 216, recante "*Disposizioni in materia di intercettazione di conversazioni o comunicazioni in attuazione della delega di cui all'art. 1, commi 82, 83 e 84, lett. a), b), c), d) ed e) della legge 23 giugno 2017, n. 103*" [126].

Prima di soffermarsi sul *novum* legislativo, è bene premettere che le regole inerenti alle intercettazioni mediante captatore informatico non trovano immediata realizzazione: dopo una serie di rimbalzi legislativi che ne hanno posposto l'attuazione[127], proprio il 31 dicembre del 2019 - nel giorno della sua ipotetica entrata in vigore[128] - il Consiglio dei Ministri modifica nuovamente la disciplina *ivi* contenuta[129], disponendo un ulteriore

---

nell'ambito del domicilio, si prevede un mero rimedio *ex post* che non impedisce l'acquisizione dell'immagine ma solo la sua utilizzabilità processuale, realizzando comunque quello che rappresenta il più incisivo *vulnus* alla sfera intima dell'individuo.

[126] Alla scadenza del terzo mese dall'entrata in vigore della legge 103 (3 agosto 2017), il Governo ottempera ai suoi doveri ed esercita il potere di delega. Il 2 novembre, infatti, il Consiglio dei Ministri vara lo schema di d.lgs. sulle intercettazioni. Dopo il parere favorevole delle Commissioni Giustizia (12 dicembre 2017, atto del Governo n. 472) e del Garante per la protezione dei dati personali (2 novembre 2017, provvedimento n. 456), lo schema diventa definitivo il 29 dicembre (G.U. 11 gennaio 2018, n. 8). Per i primi commenti al decreto in tema di intercettazioni mediante captatori, P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 235 ss.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 56 ss.; N. D'ANGELO, *La nuova disciplina delle intercettazioni dopo il d.lgs. 216/2017*, Maggioli Editore, 2017, p. 45 ss.; G. DI PAOLO, *Le intercettazioni mediante l'uso di captatore informatico*, in AA. VV., *Dai decreti attuativi della "legge Orlando" alle novelle di fine legislatura*, a cura di A. Giarda-F. Giunta-G. Varraso, Wolters Kluwer-Cedam, 2018, p. 165 ss.; M. DI STEFANO-B. FIAMMELLA, *La nuova disciplina in materia di intercettazioni. Problematicità correlate all'uso del captatore informatico*, Altalex editore, p. 89 ss.; L. GIORDANO, *La disciplina del "captatore informatico"*, cit., p. 247 ss.; R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 538 ss.; C. PARODI-N. QUAGLINO, *Il captatore informatico "entra nel sistema codicistico: un male necessario*?, in *www.ilPenalista.it*, 22 gennaio 2018; G. PESTELLI, *Brevi note sul nuovo decreto legislativo in materia di intercettazioni: (poche) luci e (molte) ombre di una riforma frettolosa*, in *Dir. pen. cont*., 2018, f. 1, p. 185 ss.; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 216 ss.; P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 119 ss.; S. SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in AA. VV., *Nuove norme in tema di intercettazioni*, cit., p. 263 ss.; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 940 s.; G. ZICCARDI, *Il captatore informatico nella ''Riforma Orlando'': alcune riflessioni informatico-giuridiche*, in *Arch. pen*., 2018, p. 497 ss.

[127] Ad eccezione di alcune disposizioni dotate di efficacia immediata (art. 6, d.lgs. n. 216/2017), l'applicazione della normativa introdotta dal d.lgs. n. 216/2017, prevista inizialmente per il 26 luglio 2018 (*ex* art. 9, comma 1, d.lgs. n. 216/2017), ha subito una serie di "rimbalzi" legislativi. La data prevista per il 31 marzo 2019 (art. 2, d.l. 25 luglio 2018, n. 91, convertito, con modificazioni, dalla l. 21 settembre 2018, n. 108), è stata prorogata al 31 luglio 2019 (art. 1, comma 1139, lett. *a)*, l. 30 dicembre 2018, n. 145) e poi rinviata al 31 dicembre 2019 (art. 9, comma 2, lett. *a)*, d.l. 14 giugno 2019, n. 53, convertito, con modificazioni, dalla l. 8 agosto 2019, n. 77).

[128] Come anticipato, l'entrata in vigore della c.d. "riforma Orlando" era prevista per il 31 dicembre 2019, a seguito dell'ennesima proroga operata dal c.d. "Decreto Sicurezza-*bis*" (d.l. n. 53/2019).

[129] D.l. 30 dicembre 2019, n. 161, recante "*Disposizioni urgenti in materia di intercettazioni*", in *Gazz. uff*., 31 dicembre 2019, n. 305, convertito, con modificazioni, dalla l. 28 febbraio 2020, n. 7, in *Gazz. uff*. 28 febbraio 2020, n. 50, su cui vedi infra § 7.

differimento dell'efficacia delle disposizioni introdotte, prima al 29 febbraio 2020[130], poi al 30 aprile 2020[131] e, infine, al 1 settembre 2020[132], con lo scopo di «consentire il completamento delle complesse misure organizzative in atto, anche relative alla predisposizione di apparati elettronici e digitali»[133].

In relazione al dettato legislativo, l'art. 4 del d.lgs. 216/2017[134], recependo i puntuali criteri direttivi contenuti nella legge delega, formalizza l'istituzione di una nuova *species* di intercettazione di comunicazioni tra presenti da condurre mediante l'immissione di captatori informatici in dispositivi elettronici portatili[135].

Facendo una riflessione di mera ingegneria normativa, la collocazione delle operazioni *de qua* stupisce lo studioso[136]. Dall'analisi dei criteri direttivi, infatti, si ipotizzava

---

[130] Più nel dettaglio, l'art. 1, comma 1, punto 1, del d.l. n. 161/2019, rinvia la decorrenza dei contenuti del decreto del 2017 (artt. 2, 3, 4, 5, 7) ai procedimenti penali iscritti dopo il 29 febbraio 2020.

[131] L. n. 7/2020, che modifica il comma 1 dell'art. 1 del d.l. n. 161/2019.

[132] D.l. 30 aprile 2020, n. 28, recante "*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*", in *Gazz. uff*., 30 aprile 2020, n. 111. Sul punto, v. M. GIALUZ, *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare*, in *Sist. pen*., 1 maggio 2020.

[133] Così *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019*, reperibile al sito *www.senato.it*. Assai critico sul punto è il CSM che, nella delibera del 13 febbraio 2020, rileva come «il breve termine previsto appaia assolutamente inadeguato, in considerazione della complessità delle misure organizzative e tecniche da adottare». Cfr. Delibera CSM, *Parere sul disegno di legge 1659 AS di conversione del d.l. 161/2019*, in *Giur. pen*. web, 17 febbraio 2020.

[134] Art. 4 del Decreto, rubricato «*Modifiche al codice di procedura penale in materia di intercettazioni mediante inserimento di captatore informatic*o».

[135] La scelta di consentire l'inserimento solo in dispositivi portatili è dovuta al fatto che proprio in riferimento a tale utilizzo dell'agente intrusore – che consente intercettazioni ubiquitarie – si sono posti nella prassi i maggiori interrogativi di compatibilità con la disciplina relativa alle intercettazioni tra presenti alla luce del "tradizionale" dovere di specifica e preventiva individuazione in seno al decreto autorizzativo dei luoghi in cui avvengono le operazioni. Cass., Sez. VI, 26 maggio 2015, Musumeci, cit. Così nessun problema si pone nel caso di infezione di un dispositivo non portatile, posto che l'attivazione del microfono garantisce comunque la sicura determinabilità del luogo in cui avvengono le captazioni. Si esprime così, D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., 217. Come sostenuto, «sembrerebbe un limite implicito di ammissibilità: il riferimento alla categoria dei *device* mobili escluderebbe l'impiego del *virus* ove il *target* fosse costituito da apparecchiature fisse […]. La scelta avrebbe un certo senso in termini di efficienza investigativa non pienamente giustificato […]. Alternativamente può ritenersi che l'inoculazione su dispositivi fissi non sia menzionata perché senz'altro consentita dalle norme generali. Ma in questo modo si rischia di legittimare un uso "libero" dei *malware*, senza le limitazioni e gli accorgimenti previsti dal decreto». Così P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 243. Si evidenzia, a tal proposito, la proposta dell'Avv. Stefano Aterno presentata presso la Commissione giustizia del Senato il 4 febbraio 2020, per cui sarebbe opportuna l'eliminazione della preclusione in esame in ragione delle attività – che ormai da diversi anni (Cfr. Cass., sez. V, 14 ottobre 2009, n. 16556, cit.) – si conducono con il captatore informatico anche sui computer fissi. Cfr. S. Aterno, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, cit.

[136] Sostengono una simile posizione D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, cit., p. 383 s.; D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*,

l'introduzione di un nuovo articolo (art. 266 *ter* c.p.p.) contenente l'intera previsione normativa; di contro, il decreto, attraverso una modifica del comma 2 dell'art. 266 c.p.p., intende attribuire all'attività in esame un preciso volto: non una nuova forma di intercettazione, da collocarsi accanto a quelle telefoniche, ambientali e telematiche, ma solo un nuovo strumento attraverso cui espletare un "vecchio" mezzo di ricerca della prova, ovvero una nuova tecnica per condurre intercettazioni ambientali.

Evidentemente il legislatore tende ad allontanarsi dall'impostazione seguita dalla giurisprudenza nel 2016. Le Sezioni Unite, infatti, avevano «circoscritto diffusamente»[137] l'orizzonte applicativo del captatore informatico. Il delegato, invece, ritiene preferibile estendere il catalogo di reati per i quali è possibile procedere alla captazione itinerante, allargando così in modo non indifferente l'ambito applicativo dell'istituto in esame rispetto al "regime pretorio" previgente.

In altri termini, a dispetto dell'impostazione contenuta delle Sezioni Unite Scurato, il delegato consente intercettazioni di comunicazioni tra presenti mediante captatore informatico non solo per i reati di criminalità organizzata – di cui inspiegabilmente restringe la portata[138] – ma anche per tutti i reati "comuni" per cui sono ritenute legittime le intercettazioni di conversazioni e comunicazioni tradizionali, ai sensi del comma 1 dell'art. 266 c.p.p.[139].

In secondo luogo, normativizzando il c.d. "doppio binario investigativo"[140], il decreto prevede che le intercettazioni di comunicazioni tra presenti mediante *virus* informatico sono sempre consentite nei luoghi di privata dimora (art. 614 c.p.), a prescindere dalla sussistenza del fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa, solo nel caso di delitti di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p.[141]; viceversa, per tutte le altre fattispecie delittuose, le captazioni mediante *virus* informatico in ambito domiciliare possono essere autorizzate solo ove sussista il sopra indicato requisito, seguendo la regolare disciplina delle intercettazioni.

---

cit., p. 557 s.; F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, cit.

[137] Così O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 59, il quale precisa che l'ambito viene "circoscritto" nel momento in cui avevano ritenuto legittimo un tale innovativo strumento di ricerca della prova per i soli delitti di criminalità organizzata; "diffusamente" perché la nozione di criminalità organizzata era tale da ricomprendere ogni delitto sussumibile nel modulo di incriminazione di cui all'art. 416 c.p.

[138] Come più volte ribadito, secondo le Sezioni Unite Scurato il riferimento ai delitti di criminalità organizzata non doveva ricondursi alle fattispecie delittuose di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., bensì doveva estendersi a qualsiasi delitto riconducibile al protocollo di tipicità oggettiva dell'art. 416 c.p.: da questo punto di vista il legislatore ha avuto il pregio di recepire quelle preoccupazioni che erano sorte in dottrina in merito a un potenziale uso eccessivo del captatore informatico.

[139] Il novellato art. 266, comma 2 c.p.p. è così strutturato: «Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile» (art. 4, comma 1, lett. *a*, punto 1 del Decreto).

[140] Art. 13, d.l. 13 maggio 1991, n. 152, cit.

[141] L'art. 266 c.p.p. viene così arricchito di un nuovo comma 2 *bis*, per cui «L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3 *bis* e 3 *quater*, (art. 4, comma 1, lett. *a*, punto 2 del Decreto).

Ulteriori novità si registrano in relazione al contenuto del decreto autorizzativo (art. 4, comma 1, lett. *b*).

Attraverso un'interpolazione del comma 1 dell'art. 267 c.p.p., si richiede al giudice procedente un ulteriore sforzo documentale per il quale il decreto assumerebbe le vesti di un provvedimento corredato da una motivazione "rafforzata". Infatti, il giudice è sempre tenuto ad indicare la ragioni che rendono necessaria la peculiare modalità operativa, valorizzando la concezione per cui il ricorso alle intercettazioni mediante captatore informatico deve essere considerata un'*extrema ratio*.

Ma si badi che la "necessità" indicata nel decreto non equivale al requisito dell'"indispensabilità" del ricorso al particolare strumento investigativo che, per converso, non è richiesto dal dato normativo, ovvero «il giudizio di necessità non coincide con quello di certa infruttuosità delle altre forme di intercettazione ambientale quanto piuttosto con la prova […] di una meno agevole praticabilità delle operazioni tradizionali»[142].

In sostanza, dal tenore letterale della disposizione in esame si evince che non è necessaria la prova del fatto che il ricorso a tale peculiare forma di intercettazione sia l'unico strumento operativo praticabile; tuttavia, come precisato, «[P]pare comunque evidente che la necessità deve riguardare il *quomodo* dell'intercettazione; essa deve consistere in un giudizio di congruità tra la tecnica esecutiva ed il particolare contesto investigativo contingente nel quale si deve andare ad operare per svolgere proficuamente le indagini»[143].

Nel caso in cui si proceda per delitti diversi da quelli indicati nell'art. 51, commi 3 *bis* e 3 *quater*, gli adempimenti motivazionali si aggravano ulteriormente, dovendo il giudice indicare anche «i luoghi e il tempo, […] in relazione ai quali è consentita l'attivazione del microfono»[144].

A questo proposito, il legislatore delegato, ben consapevole della difficoltà di prevedere nel dettaglio gli spostamenti di un dispositivo portatile e, di conseguenza, di indicare nel decreto autorizzativo i tempi e i luoghi in cui attivare il microfono per la captazione audiofonica, introduce la facoltà di una determinazione anche "indiretta" dei luoghi in cui è possibile intercettare conversazioni e comunicazioni[145] nonché la sanzione

---

[142] D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 219.

[143] Così Relazione dell'Ufficio del Massimario della Corte di Cassazione sulla *legge 28 febbraio 2020, n. 7, conversione in legge con modificazioni del decreto legge 30 dicembre 2019, n. 161, Modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*, n. 35, 23 marzo 2020, p. 8 s.

[144] Il comma 1 dell'art. 267 c.p.p. viene così arricchito di un ulteriore periodo: «Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3 *bis* e 3 *quater*, i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono» (art. 4, comma 1, lett. *b*, punto 1 del Decreto).

[145] Sul punto la relazione illustrativa allo schema di decreto legislativo indica che la scelta di consentire una determinazione anche indiretta dei luoghi si spiega nell'impossibilità di prevedere specificamente tutti gli spostamenti dell'apparecchio controllato, con conseguente necessità logica di delimitare gli ambiti ai verosimili spostamenti del soggetto, in base alle emergenze investigative. A titolo esemplificativo la relazione indica che è legittimo quindi fare ricorso a formule del tipo "ovunque incontri il soggetto x" oppure "ogni volta che si rechi nel locale y" e così via. Cfr. CdM, *Relazione illustrativa allo schema di decreto legislativo*, in *www.documenti.camera.it.*

dell'inutilizzabilità nel caso di dati illegittimamente acquisiti (art. 271, comma 1 c.p.p.)[146].

Di qui, la dottrina si chiede quale debba essere il livello di precisione richiesto al gip per l'indicazione anche indiretta, dei luoghi e del tempo[147], dal momento che una indicazione eccessivamente meticolosa rischia di rendere inutile lo strumento investigativo, mentre l'indeterminatezza totale del decreto renderebbe la tecnica captativa *ad explorandum* e dunque inutilizzabile.

A prescindere dal fatto che la giurisprudenza si è sempre mostrata assai indulgente nei casi di variazione *in itinere* dei luoghi oggetto di intercettazione[148], in assenza di pronunce giurisprudenziali chiarificatrici, si può immaginare che saranno impiegate formule generali ampie per valutare la precisione della delimitazione spaziale, le quali di per sé non possono assumere un significato precettivo se non calate nell'orizzonte specifico della fattispecie concreta[149].

Assai più innovativa appare la previsione della determinazione temporale in relazione alla quale è consentita l'attivazione del microfono sul dispositivo.

Nel rispetto del termine massimo di durata delle intercettazioni, il giudice deve indicare i tempi nei quali è permessa la captazione a mezzo di *virus* informatico e, conseguentemente, quando è ammissibile l'attivazione del microfono.

Si delinea, in tal modo, un sistema assai diverso rispetto a quello previsto per le "tradizionali" forme di intercettazioni, ove la captazione di conversazioni e comunicazione (ovvero di dati) è permanente per tutta la durata delle operazioni nel rispetto dei limiti dettati dal decreto.

In questo caso, invece, fissata la durata complessiva delle operazioni, gli ascolti avverranno in ragione di specifiche occasioni preventivamente determinate; così i tempi di registrazione «saranno individuati in ragione di due differenti variabili, l'una relativa all'arco temporale delle operazioni e l'altra in ragione delle singole occasioni di vera e propria captazione»[150].

Poi, attraverso l'introduzione di un nuovo comma 2 *bis* all'art. 267 c.p.p., il ruolo di protagonista indiscusso del p.m. nell'ambito della procedura d'urgenza viene attenuato: lo stesso, infatti, può procedere ad autorizzare l'esecuzione delle operazioni mediante *virus* informatico con decreto motivato – che dovrà menzionare le specifiche ragioni

---

[146] Nel previgente regime, dal momento che l'indicazione del tempo e del luogo non erano espressamente annoverati tra i presupposti del provvedimento, la sanzione dell'inutilizzabilità non era comminabile. Il rimando operato dall'art. 271 c.p.p. all'art. 267 c.p.p. deve oggi considerarsi esteso interamente a questo ultimo articolo.

[147] C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in *Dir. pen. cont.*, 13 aprile 2018, p. 24 s.; M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, cit., p. 40; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 219 ss.

[148] La Suprema Corte ha mostrato un'apertura al "carattere dinamico" dell'attività di controllo in riferimento ai diversi ambienti potenzialmente frequentabili dal soggetto ad esso sottoposto. Da ultimo cfr. Cass., sez. IV, 3 febbraio 2016, n. 4484, in *www.processopenaleegiusitizia.it.*

[149] In questo senso O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 62.

[150] D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., 221.

dell'urgenza, tali da non permettere l'attesa del naturale provvedimento giurisdizionale – solo nel caso di reati di cui all'art. 51, commi 3 *bis* e 3 *quater*[151].

Inoltre, al fine di attuare "un monitoraggio del monitorante", il decreto attribuisce la titolarità dell'attivazione e della cessazione delle operazioni all'ufficiale di polizia giudiziaria, ovvero ad un ausiliario esterno[152]. Il riferimento va ai tecnici delle società private esterne che gestiscono il servizio e che collaborano con la p.g. nella complessa fase di inoculazione e disinstallazione del *virus* nella macchina bersaglio. In sostanza, così come già indicato nella delega, da mera attività "automatizzata", la captazione diventa un'azione «a uomo presente»[153].

In relazione, invece, ai profili "tecnici" – peculiarità indiscussa della delega governativa – l'art. 89 disp. att. c.p.p. viene arricchito di una serie di commi deputati a regolamentare il contenuto del verbale delle operazioni di p.g., il tipo di programmi da utilizzare nonché le cautela da rispettare al fine di garantire l'integrità della catena di custodia[154].

In particolare, il verbale di intercettazioni dovrà indicare i nominativi dei soggetti delegati alle operazioni, l'ora di inizio e fine delle operazioni nonché il tipo di programma impiegato e i luoghi oggetto di captazione (comma 1). Si prevede, inoltre, che ai fini dell'istallazione e dell'intercettazione mediante captatori informatici possano essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministero della giustizia (comma 2 *bis*)[155].

Una volta intercettate, le comunicazioni sono trasferite esclusivamente verso gli impianti della Procura della Repubblica e, durante il trasferimento, sono operati costanti controlli di integrità del dato in modo da assicurare la conformità tra lo stesso e quanto trasmesso e registrato (comma 2 *ter*). Se, tuttavia, appare impossibile procedere al

---

[151] Nei casi di cui al comma 2, il pubblico ministero può disporre, con decreto motivato, l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile soltanto nei procedimenti per i delitti di cui all'articolo 51, commi 3 *bis* e 3 *quater*. A tal fine indica, oltre a quanto previsto dal comma 1, ultimo periodo, le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice. Il decreto è trasmesso al giudice che decide sulla convalida nei termini, con le modalità e gli effetti indicati al comma 2» (comma 2 *bis* dell'art. 267, introdotto *ex* art. 4, comma 1, lett. *b*, punto 2 del Decreto).

[152] «Per le operazioni di avvio e di cessazione delle registrazioni con captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, comma 4» (comma 3 *bis*, art. 268, introdotto *ex* art. 4, comma 1, lett. *c* del Decreto). Degno di nota è l'emendamento n. 35.133 (relatori Orellana, Battista) teso da un lato ad eliminare i profili più critici della disciplina come la possibilità che le intrusioni vengano effettate da personale esterno alle forze di polizia, nelle forme dell'art. 348 comma 4 c.p.p., e dall'altro a potenziare le garanzie difensive prevedendo che «al termine delle indagini, sia dato il diritto alla difesa di ottenere la documentazione relativa a tutte le operazioni eseguite tramite captatori, dall'installazione fino alla loro rimozione, nonché la possibilità di chiedere al giudice di verificare che il captatore utilizzato rispetti i requisiti previsti dalla normativa vigente».

[153] In questo senso C. PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici*", cit.

[154] Art. 5 del Decreto.

[155] Il Decreto ministeriale di cui al comma 7 del d.lgs. 216/2017 è stato emanato. Cfr. D.m. 20 aprile 2018, recante "*Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216*", Bollettino ufficiale del Ministero della Giustizia, 31 maggio 2018, n. 10.

contestuale trasferimento dei dati intercettati, il verbale dovrà anche indicare le ragioni tecniche impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate (comma 2 *quater*).

Infine, viene espressamente previsto l'onere per l'ufficiale di p.g. ovvero del personale di cui si è avvalso ai sensi dell'art. 348 c.p.p., di disattivare il captatore, dandone atto nel verbale (comma 2 *quinquies*).

Forse eccessiva la superficialità con cui il legislatore dispone la disinstallazione – e la conseguente distruzione – del dispositivo. Ed infatti, come rilevato dai "tecnici", la disinstallazione degli stessi dalla macchina bersaglio porrebbe non pochi problemi di ordine pratico: dovendo questa avvenire necessariamente da remoto, potrebbero perdersi le tracce e il controllo stesso del *virus*, banalmente perché il dispositivo elettronico non si connette più alla rete, permettendo, dunque, un monitoraggio "perenne" dello stesso, che travalica le finalità per cui viene autorizzato.

Nel complesso, si tratta di un «modesto ritocco»[156] apportato dal legislatore delegato che, nonostante gli originali propositi, finisce per «scontentare tutti»[157], dal momento che non sembra improntato alla tutela del diritto di difesa né dell'imputato né della persona offesa dal reato.

5.1. *SEGUE*: I DIVIETI DI UTILIZZAZIONE DEL CAPTATO

La riforma tocca anche la disciplina dei divieti di utilizzazione probatoria dei dati illegittimamente appresi (artt. 270 e 271 c.p.p.)[158].

Tali modifiche – seppur non definitive[159] – appaiono assai interessanti in quanto tese a garantire una concreta, effettiva e più esplicita tutela del diritto di riservatezza, in conformità alla *ratio* che ha ispirato il repentino intervento riformatore.

Ai sensi del nuovo comma 1 *bis* dell'art. 270 c.p.p. viene prevista l'inutilizzabilità dei dati raccolti mediante captatore informatico per la prova di reati diversi da quelli per cui è stato emesso il decreto autorizzativo, «salvo che gli stessi siano necessari per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio»[160].

---

[156] L. FILIPPI, *Pubblicata in gazzetta la riforma delle intercettazioni*, in *www.quotidianogiuridico.it,* 12 gennaio 2018, p. 7.

[157] Si esprime così L. FILIPPI, *Pubblicata in gazzetta la riforma delle intercettazioni*, cit., p. 7.

[158] Sul tema, approfonditamente, T. ALESCI, *Le intrusioni* inter praesentes, in AA. VV., *L'intercettazione di comunicazioni*, cit., p. 82 ss.; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 257 ss.; ID., *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 330 ss.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 73 ss.; F. CASSIBBA, *La circolazione delle intercettazioni tra "archivio riservato" e captatore informatico",* in AA. VV., *Le nuove intercettazioni*, cit., p. 163 ss.

[159] Si precisa che la normativa subisce numerosi rimaneggiamenti ad opera degli interventi legislativi successivi, fino a stravolgere completamente il suo significato iniziale. Sul punto, v. § 6 e 7.

[160] Art. 4, comma 1, lett. *d* del Decreto. In tal modo il governo ha dato seguito, non senza alcune imprecisioni, alla delega parlamentare che imponeva, all'art. 1, comma 84, lett. e, n. 7, l. 103/2017, che «i risultati intercettativi così ottenuti po[tesser]o essere utilizzati ai fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e po[tesser]o essere utilizzati in procedimenti diversi a

Prima facie, la scelta del delegato appare assolutamente condivisibile[161]. La sostituzione del termine "procedimenti" – utilizzato nel primo comma dell'art. 270 c.p.p. – con "reati", impone un'interpretazione maggiormente rigorosa del *dictum*, escludendo, per queste nuove forme captative, la possibilità di impiegare i risultati dell'attività investigativa per tutti le altre fattispecie criminose di cui, per il tramite dell'intercettazione, emergano gli estremi[162]: in sostanza, se con il disposto dell'art. 270, comma 1 c.p.p., la «disciplina eccezionale»[163] scatta purchè il procedimento sia diverso, ai sensi del comma 1 *bis* dell'art. 270 c.p.p., interviene purchè il reato sia diverso[164].

Inoltre, la formulazione del nuovo comma 1 *bis* dell'art. 270 c.p.p. rende assai difficile ritenere utilizzabile l'intercettazione anche in ipotesi di successiva riqualificazione del reato oggetto di indagine, salvo che per il caso in cui il mutamento del titolo conduce ad una imputazione rientrante nell'elenco dei reati "gravi", di cui all'art. 380 c.p.p.[165].

Come, tuttavia, dimostrano orientamenti giurisprudenziali consolidati in materia[166], pur non potendoli utilizzare per scopi processuali, gli stessi potrebbero essere impiegati

---

condizione che siano indispensabili per l'accertamento dei delitti di cui all'articolo 380 del codice di procedura penale». Secondo parte della dottrina «tale formulazione aveva suscitato qualche perplessità, soprattutto in riferimento alla prima statuizione, poiché l'attuazione di tale criterio avrebbe potuto determinare un doppio binario in tema di inutilizzabilità» Così T. ALESCI, *Le intrusioni* inter praesentes, cit., p. 83. Preoccupazioni che si sono poi in effetti rivelate fondate, se si tiene in considerazione che i risultati intercettivi ubiquitari non possono essere utilizzati per la prova di reati di diversi e non, come prescrive l'art. 270, comma 1, c.p.p., in procedimento diversi. In questo senso O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 74.

[161] G. AMATO, *Per l'uso del* "trojan" *compromesso non facile sulle regole*, cit., p. 55; F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, cit., p. 369. *Contra*, A. TESTAGUZZA, voce Virus *informatico,* cit., p. 940, per cui «[I]il rischio […] è che si possano […] aggirare gli stringenti vincoli imposti dal sistema per l'impiego dell'apparato, mediante l'uso dei risultati probatori acquisiti al di là del catalogo dei reati che ne avrebbe legittimato l'adozione».

[162] In effetti, fino alla fatidica pronuncia delle Sezioni unite del 2019 (Cass., sez. un. 28 aprile 2019, n. 51, in *Sist. pen*., 2020, 30 gennaio 2020) la giurisprudenza maggioritaria stratificatisi in materia di inutilizzabilità *extra* procedimentale dei risultati intercettivi tendeva ad ammetterne l'impiego per la prova dei reati diversi emersi nel corso di quello stesso procedimento, a prescindere dalle condizioni poste dall'art. 270, comma 1 c.p.p. (Cass., sez. VI, 21 febbraio 2018, n. 19496, in *C.E.D. Cass.,* n. 273277; sez. VI, 26 aprile 2017, n. 31984, *ivi*, n. 270431; sez. V, 16 marzo 2016, n. 45535, *ivi*, n. 268453; sez. IV, 8 aprile 2015, n. 29907, *ivi*, n. 264382) e, talvolta, anche a prescindere dalla loro inclusione nell'elenco dei reati intercettabili ex art. 266, comma 1 c.p.p. (sez. fer., 23 agosto 2016, n. 355336, *ivi*, n. 267598). Sulla complessa *querelle* dottrinale e giurisprudenziale in tema di usi obliqui dei risultati delle intercettazioni, si consenta un rinvio a Cap. II, Parte II, § 5.

[163] Nel senso che l'art. 270 c.p.p. abbia natura eccezionale, A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 271 s. Conformemente G. DI CHIARA, *Note in tema di circolazione di atti investigativi e probatori in procedimenti diversi,* in *Foro it.,* 1992, f. 2, p. 78 s.

[164] Sottolinea la creazione di «ingiustificato doppio binario», L. PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni,* in *Dir. pen. cont.* 2018, f. 1, p. 64.

[165] In questo senso T. ALESCI, *Le intrusioni* inter praesentes, cit., p. 83; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 261; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 226; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 126 ss.;

[166] Cass., sez. II, 13 dicembre 2016, n. 17759, in *C.E.D. Cass*., n. 270219; sez. II, 23 aprile 2010, n. 19699, *ivi,* n. 247104; sez. V, 2 maggio 2003, n. 23894, *ivi,* n. 225946.

per "formare" la notizia di reato[167]. E allora, si potrebbe ipotizzare che la scelta del legislatore di riferirsi all'intero "procedimento" sia funzionale ad estendere l'ambito del divieto anche alla fase delle indagini preliminari, precludendone l'utilizzo anche nel primo *step* dell'intera procedura, arginando una prassi deviata caratterizzata da iscrizioni affrettate nel registro, *ex* art. 335 c.p.p., per reati che permetterebbero il ricorso all'intercettazione, sebbene poi il prosieguo del procedimento evidenzi la necessità di pervenire ad una derubricazione[168].

Su un altro versante, precisando maggiormente i troppo vaghi criteri direttivi contenuti nella delega[169], la sanzione dell'inutilizzabilità viene estesa anche al caso di dati acquisiti *ultra vis*, ai sensi del novello comma 1 *bis* dell'art. 271 c.p.p.[170]: in particolare, non sono utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e sono parimenti inutilizzabili i dati acquisiti al di fuori dei limiti spazio-temporali indicati nel decreto autorizzativo.

Sicuramente una volontà apprezzabile quella di introdurre un rimedio sanzionatorio processuale alla disattenzione del divieto, ma, probabilmente, inefficace sul piano fattuale. Al fine di rendere effettivo l'impedimento, infatti, sarebbe stato opportuno prevedere espressamente – anche con un richiamo all'art. 115 c.p.p. – una sanzione contro l'illegittima divulgazione di atti che risultano, *tout court*, coperti da segreto[171].

5.2. *SEGUE*: IL "TERZO BINARIO" INVESTIGATIVO PER I REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

Con riferimento ai procedimenti per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione, ossia quelli puniti con la pena della reclusione non inferiore nel massimo a cinque anni[172], determinata a norma dell'art. 4 c.p., l'art. 6 del d.lgs.

---

[167] Sul tema della pre-inchiesta si rinvia a R. APRATI, La notizia di reato nella dinamica del procedimento penale, Jovene, Jovene, 2010, p. 60 ss.; A. MARANDOLA, I registri del pubblico ministero, Cedam, 2001, p. 70 ss.; A. ZAPPULLA, La formazione della notizia di reato, Giappichelli, 2012, p. 248 ss.

[168] Una simile posizione è accolta da G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione*, p. 139 ss. Critico sul punto D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 226.

[169] Secondo cui i risultati delle intercettazioni «che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede non possono essere conoscibili, pubblicabili e, dunque, divulgabili».

[170] Art. 4, comma 1, lett. *e* del Decreto.

[171] In questo senso O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 74.

[172] La disciplina, che richiama implicitamente l'art. 266, comma 1, lett. b) c.p.p., si applica quindi ai delitti previsti e puniti dagli artt. 314, comma 1, 317, 318, 319, 319 *ter*, 319 *quater*, 320, 321, 322, 322 *bis*, 325 e 326, comma 3, primo periodo, c.p. Giusto il caso di sottolineare che, in realtà, l'art. 266 richiamato, nel prevedere alla lett. b) una disciplina più favorevole all'impiego delle intercettazioni di quella disposta in via ordinaria alla precedente lett. a), rimanda genericamente ai reati contro la pubblica amministrazione; sarebbe stato quindi preferibile estendere la nuova normativa quantomeno anche ai delitti, ricompresi tra quelli commessi dai privati contro la pubblica amministrazione, di cui agli artt. 353, 353 *bis* e 356 c.p. Peraltro, la giurisprudenza ritiene che la valutazione del reato per il quale si procede, da cui dipende l'applicazione della disciplina ordinaria

216/2017 introduce una disciplina alquanto particolare, delineando un "terzo binario" investigativo (che si affianca a quello che previsto per i reati di criminalità organizzata e terrorismo)[173] per le intercettazioni mediante captatore informatico[174].

In particolare, il comma 1 dell'art. 6 del decreto prevede che per tali procedimenti, «si applicano le disposizioni di cui all'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203», tentando una semplificazione per le condizioni di impiego del prezioso strumento investigativo[175]; tuttavia, qualora la captazione avviene nei luoghi indicati dall'articolo 614 c.p.[176], «non può essere eseguita mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa».

Si potrebbe parlare di disciplina bipartita che riprende alcune previsioni "speciali" in tema di lotta alla criminalità[177] ed esclude la normativa derogatrice in favore di quella impiegata per i reati comuni qualora la captazione avviene nei luoghi di privata dimora, di cui all'art. 614 c.p.

Detto in altri termini, secondo il modello introdotto nel 2017[178], per queste fattispecie di reato si prefigura una disciplina «ibrida»[179], a «mezza via»[180] tra quella prevista per le intercettazioni "ordinarie" e quelle "speciali", che risente della parificazione tra i reati

---

ovvero quella speciale per la criminalità organizzata va fatta con riguardo all'indagine nel suo complesso e non con riferimento alla responsabilità di ciascun indagato (cfr. Cass., sez. VI, 6 aprile 2017, n. 28252, in *C.E.D. Cass*., n. 270565; sez. V, 4 marzo 2016, n. 26817, *ivi*, n. 267889): l'orientamento appare certamente estensibile anche ai reati contro la pubblica amministrazione, anche in considerazione del fatto che l'art. 6, comma 1, del decreto in esame fa rifermento ai "procedimenti" per i reati di pubblica amministrazione e non alle singole ed autonome posizioni di coloro che, a vario titolo, vengono coinvolti nell'indagine.

[173] Per una ricostruzione del concetto di "criminalità organizzata", v. G. MELILLO, *La ricerca della prova tra clausole generali e garanzie costituzionali: il caso della disciplina delle intercettazioni nei procedimenti relativi a delitti di criminalità organizzata,* in *Cass. pen*., 1997, f. 1, p. 350 ss.

[174] Sul tema, v. P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 255 ss.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 65 s.; P. MAGGIO, *I presupposti applicativi,* in AA. VV., *L'intercettazione di comunicazioni,* cit., p. 46 ss.; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 226 ss.; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 134; G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione*, cit., p. 139 ss.; F. RUGGIERI, *Le deroghe alla disciplina codicistica, in* AA. VV., *L'intercettazione di comunicazioni*, cit., p. 95 ss.

[175] In ossequio a quanto previsto dalla legge "Orlando" nell'art. 1, comma 84, lett. d), il decreto avrebbe dovuto prevedere una «semplificazione delle condizioni per l'impiego delle intercettazioni telefoniche e telematiche nei procedimenti per i reati più gravi dei pubblici ufficiali contro la pubblica amministrazione». Sul tema, esaustivamente, L. FILIPPI, *La legge delega sulle intercettazioni*, in AA. VV., *Le recenti riforme in materia penale*, cit., p. 7 ss.

[176] Sul concetto di "privata dimora", si rinvia a nt. 61.

[177] Art. 13, d.l. 152 del 1991, cit. Cfr. A. TESTAGUZZA, voce Virus *informatico*, cit., p. 941.

[178] Anche in questo caso, proprio come per i divieti di utilizzo extraprocedimentale del captato, la disciplina subisce ingenti modifiche ad opera della legislazione successiva. Cfr. § 6 e 7.

[179] Così F. RUGGIERI, *Le deroghe alla disciplina codicistica*, cit., p. 95 ss.

[180] La definisce così D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 228.

gravi contro la pubblica amministrazione e quelli distrettuali, pur caratterizzandosi per una sua peculiarità.

Per comprendere a fondo la modifica operata, occorre ripartire dalla disciplina delineata dall'art. 13 del d.l. 152 del 1991 in relazione alle intercettazioni per i procedimenti per reati di criminalità organizzata e terrorismo. In questi casi, non occorrono "gravi indizi" di reato, né l'affermazione dell'"indispensabilità" del ricorso all'intercettazione, ma semplicemente "sufficienti indizi" e la mera "necessità" della captazione. La durata massima delle operazioni è differente rispetto a quella ordinaria (40 giorni, prorogabili di 20) e, laddove l'intercettazione si svolga in luoghi di privata dimora, non occorre la sussistenza del requisito di cui al comma 2 dell'art. 266 c.p.p.[181].

Se tutti i requisiti anzi detti valgono anche per le intercettazioni disposte nei procedimenti contro la pubblica amministrazione, quest'ultima previsione non trova applicazione allorquando la captazione avviene mediante l'inoculazione di un captatore informatico su un dispositivo elettronico portatile, non potendosi ammettere intercettazioni ambientali domiciliari quando non vi sia "motivo" (anche se non fondato) di ritenere che in quel luogo si stia svolgendo l'attività criminosa.

Volendo semplificare: l'intercettazione tra presenti nei luoghi di privata dimora, in tema di più gravi reati dei pubblici ufficiali contro la pubblica amministrazione, può essere liberamente eseguita utilizzando le tradizionali forme captative mediante sonde da collocare fisicamente nei luoghi monitorandi; al contrario, è limitata alla sussistenza di fondati motivi di ritenere che in quei luoghi si stia svolgendo l'attività criminosa, qualora si intenda operare l'ascolto mediante l'attivazione del microfono di un dispositivo elettrico portatile.

Non solo. Tale disciplina, valevole per i reati dei pubblici ufficiali contro la pubblica amministrazione, appare estensibile anche ai procedimenti comunque facenti capo ad un'associazione per delinquere seppur diversa da quelle richiamate all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., per i quali, da un lato, si applicano le disposizioni di cui all'art. 13 del citato d.l. n. 152/1991 in forza di quanto indicato dalla giurisprudenza di legittimità nel 2016[182] ma dall'altro non si applica la più estensiva disciplina del nuovo comma 2 *bis* dell'art. 266 c.p.p. che fa esclusivo richiamo a specifiche fattispecie delittuose.

Secondo alcuni autori, la scelta *de qua* si rivela alquanto infelice, oltre che infruttuosa[183]. A ben guardare, infatti, l'equiparazione tra i reati gravi contro la pubblica amministrazione e i reati distrettuali non è priva di una sua plausibilità: se per la criminalità organizzata il potenziamento delle prerogative investigative corrisponde, oltre che alla spiccata gravità, alla maggior difficoltà di indagine ed accertamento, legata al carattere "organizzato" di queste fenomenologie criminose, per i reati contro la pubblica amministrazione la regole della eguale incriminabilità dei partecipi all'accordo criminoso costituisce per le inchieste penali uno schermo assai difficilmente penetrabile senza

[181] Per una panoramica della peculiarità della normativa introdotta, si rinvia a nt. 66.

[182] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[183] Come precisato dalla dottrina, «si tratta di una scelta "controcorrente" quella di indicare per via *negationis* possa o non possa essere utilizzato e che si pone in netto contrasto con quanto originariamente previsto nella prima bozza». Così A. TESTAGUZZA, voce Virus *informatico*, cit., p. 941. Nello stesso senso D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni,* cit., p. 227.

violare la segretezza delle comunicazioni[184]. Di conseguenza, per questo tipo di reati accade spesso che sia fondamentale per le indagini «procedere agli ascolti delle conversazioni che avvengono, a commento di altri incontri o conversazioni difficilmente monitorabili, nei luoghi di lavoro o addirittura nelle abitazioni»[185].

L'aver previsto un «regime intermedio»[186] applicabile sia ai procedimenti inerenti ai reati "gravi" contro la pubblica amministrazione, sia per quelli facenti capo a un'associazione per delinquere estromessa dalla disciplina derogatoria di cui all'art. 266, comma 2 *bis* c.p.p., sembra non del tutto inadeguata a fronte della peculiarità di tali fattispecie delittuose, per cui la necessità di effettuare captazioni ambientali domiciliari "libere" sembra dover essere prioritaria rispetto alla tutela domiciliare.

Secondo altri, invece, «[L]l'appiattimento del legislatore sul modulo di cui all'art. 13 d.l. 152/1991 conferma la deriva verso modalità intercettative ben lontane dall'offrire quel necessario ragionato bilanciamento tra esigenze investigative e diritti fondamentali […], denunciando la perdita di centralità di un sistema differenziato per ciascuna tipologia di reato»[187].

6. Il progressivo ampliamento delle fattispecie intercettabili. La legge "Spazzacorrotti"

Il biennio 2017-2019 si profila assai complesso sul fronte del contrasto al «morbo della corruttela»[188]: un susseguirsi ininterrotto di pronunce giurisprudenziali ondivaghe[189] e scandali giornalistici travolgenti i più importanti esponenti della magistratura nazionale[190] dimostrano l'inidoneità della normativa vigente a reprimere il fenomeno, richiedendo un intervento impellente del legislatore.

La «giustizia vendicativa gialloverde»[191] che fonda la sua politica sul populismo penale, «strumentalizza[ndo] le paure e le angosce della gente comune […]»[192], crea un terreno fertile per imporre logiche emergenziali sempre più tese ad accrescere la repressione e a restringere gli spazi del garantismo. In questo contesto, la criminalità dei

---

184 In questo senso P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 255; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*¸ cit., p. 227.

185 D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 227.

186 L'espressione appartiene a P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 256.

187 Così F. RUGGIERI, *Le deroghe alla disciplina codicistica*, cit., p. 109.

188 Così M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 388.

189 Cfr., Cass., sez. VI, 13 giugno 2017, n. 36874, cit.

190 Solo a titolo esemplificativo ci si può riferire all'indagine della Procura di Perugia nei confronti dell'*ex* Presidente dell'ANM (Associazione Nazionale Magistrati) ed *ex* consigliere del CSM Luca Palamara. Quell'indagine rappresenta una delle prime inchieste italiane in cui il *Trojan* viene utilizzato per reati contro la pubblica amministrazione. Il caso, assai delicato per le sue innumerevoli implicazioni, è rilevante anche in ragione della quaestio relativa all'inutilizzabilità dei risultati intercettivi per la prova di reati diversi da quelli per cui si procede.

191 La definisce così E. AMODIO, *A furor di popolo. La giustizia vendicativa gialloverde*, Donzelli Editore, 2019, p. VII.

192 Così E. AMODIO, *A furor di popolo. La giustizia vendicativa gialloverde*, cit., p. 13.

c.d. colletti bianchi diventa la «nuova emergenza»[193] da affrontare nell'attuale contingenza storica[194]; un fenomeno complesso che, affondando le sue radici nel substrato culturale e nelle abitudini sociali[195], risulta assai difficile da scardinare.

Di qui, l'esigenza di una riforma travolgente in un settore già vessato da riforme compulsive, volta non tanto e non solo ad inasprire la risposta sanzionatoria ma anche e soprattutto a facilitare l'impiego di tecniche investigative inedite che agevolino l'operato degli inquirenti, nella convinzione per cui l'effettività della legge penale non dipende solo dalle norme incriminatrici ma anche dall'ampiezza dell'incisività degli strumenti di indagine impiegabili.

La risposta non tarda ad arrivare. Con la l. 9 gennaio 2019, n. 3 (c.d. legge "Spazzacorrotti" o "anticorruzione")[196], il legislatore introduce svariate misure, volte ad «affrontare in modo efficace il fenomeno corruttivo e, in generale, per assicurare una maggiore incisività all'azione di contrasto dei reati contro la pubblica amministrazione»[197].

La riforma opera lungo due linee direttrici: sia sul piano del diritto penale sostanziale, specialmente tramite l'inasprimento sanzionatorio in relazione a talune specifiche tipologie delittuose e la previsione di una più severa disciplina delle pene accessorie, sia sotto il profilo investigativo e processuale, con la modifica di alcune disposizioni del codice di procedura penale e della l. 16 marzo 2006, n. 146, in tema di operazioni sotto copertura[198].

Per quel che in questa sede rileva, il legislatore blinda l'opzione investigativa del ricorso al captatore informatico per effettuare intercettazioni di conversazioni tra presenti qualora si proceda per i delitti dei pubblici ufficiali contro la pubblica amministrazione

---

[193] V. MONGILLO, *La legge "Spazzacorrotti": ultimo approdo del diritto penale emergenziale nel cantiere permanente dell'anticorruzione*, in *Dir. pen. cont*., 27 maggio 2019.

[194] Sul rapporto tra la legislazione anticorruzione ed emergenza, si rinvia a M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 27 ss. Più in generale, v. G. INSOLERA, *L'evoluzione della politica criminale tra garantismo ed emergenze. Dagli anni '60 all'emergenza mafiosa*, in *Riv. it. dir. proc. pen*., 2014, f. 3, p. 1165 ss.; G. RICCIO, voce *Emergenza*, in *Dizionario di diritto e procedura penale*, a cura di G. Vassalli, Giuffrè, 1986, p. 281 ss.; ID., *Politica penale dell'emergenza e costituzione*, Napoli, 1982; G. SPANGHER, *Processo penale: le nuove emergenze*, in *Cass. pen*., 2015, f. 9, p. 2994 ss.; ID., *Considerazioni sul processo "criminale" italiano*, cit., p. 7 ss.

[195] In questo senso S. DE SANTIS, *L'uso politico degli strumenti processuali penali*, in *Arch. pen.,* 2013, f. 2, p. 2 ss.

[196] L. 9 gennaio 2019 n. 3, recante «*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*», in *Gazz. uff.,* 16 gennaio 2019, n. 13.

[197] Cfr. *Relazione di accompagnamento al Disegno di legge n. 1189*, presentato alla Camera il 24 settembre 2018 dal Ministro della Giustizia Bonafede, reperibile sul sito *www.camera.it.*

[198] Per una prima analisi delle principali novità, A. DE VITA, *La nuova legge anticorruzione e la suggestione salvifica del Grande Inquisitore. Profili sostanziali della l. 9 gennaio 2019, n. 3*, in *Proc. pen. giust.,* 2019, f. 4, p. 947 ss. V. MANES, L'estensione *dell'art. 4*-bis *ord. pen. ai delitti contro la p.a.: profili di illegittimità costituzionale*, in *Dir. pen. cont.*, 2019, f. 2, p. 105 ss.; T. PADOVANI, *La spazzacorrotti. Riforma delle illusioni e illusioni della riforma,* in *Arch. pen*., 2018, 1 ss. Con precipuo riguardo all'ambito processuale, v. A. CAMON, *Disegno di legge spazzacorrotti e processo penale. Osservazioni a prima lettura*, in *Arch. pen*., 2018, f. 3, p. 1 ss.; A. DE CARO, *La legge c.d. spazza corrotti: si dilata ulteriormente la frattura tra l'attuale politica penale, i principi costituzionali e le regole del giusto processo*, in *Proc. pen. giust*., 2019, f. 2, p. 281 ss.

puniti con la reclusione non inferiore nel massimo a cinque anni[199], forte della convinzione per cui «il contrasto al fenomeno corruttivo non si realizza esclusivamente sul piano del diritto sostanziale […] ma anche attraverso la semplificazione dei presupposti richiesti dalla legge per l'impiego di […] efficaci tecniche di investigazione»[200].

L'intervento mira in sostanza a completare quel percorso di equiparazione tra i "gravi" contro la pubblica amministrazione e i reati distrettuali in ragione della spiccata gravità che sembra connotare gli specifici reati presi in considerazione dalla normativa di recente approvazione.

Sul piano operativo, gli artt. 2 e 3, lett. *a* e *b*, del disegno di legge "spazza-corrotti", poi confluiti, inalterati nel loro contenuto, nell'art. 1, commi 3 e 4, lett. *a* e *b* della l. n. 3/2019, incidono sull'assetto normativo delineato dagli artt. 266, comma 2 *bis* e 267, comma 1 c.p.p., estendendo il campo applicativo della disciplina "speciale" sulle intercettazioni eseguite mediante inserimento del captatore informatico, precedentemente contemplata (soltanto) per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., anche ai reati dei pubblici ufficiali contro la pubblica amministrazione[201], puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p.

Più precisamente, abrogando il comma 2 dell'art. 6 del d.lgs. 216/2017 e modificando il comma 2 *bis* dell'art. 266 c.p.p., si prevede l'estensione della disciplina derogatoria prevista per i delitti di criminalità organizzata, alla categoria dei reati contro la pubblica amministrazione, puntualmente individuati sulla base del criterio relativo all'entità del massimo edittale, sancendo che anche per questi ultimi è «sempre consentito l'uso del captatore informatico» e, di conseguenza, anche per eseguire intercettazioni ambientali domiciliari a prescindere dal fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa.

Coerentemente con tale impostazione, la legge interviene anche sull'art. 267 c.p.p., in relazione ai presupposti del provvedimento autorizzativo per effettuare operazioni di intercettazione, prevedendo che la deroga alla motivazione "rafforzata" possa essere prevista – oltre che per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p. – anche per i delitti corruttivi[202].

---

[199] Per commenti, L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico,* in *Dir. pen. cont*., 24 settembre 2019; M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 388 ss.; A. MARANDOLA, *L'inasprimento del regime dei reati contro la P.A. (c.d. Spazzacorrotti),* in *Studium Iuris*, 2019, f. 10, p. 1159 ss.; S. SIGNORATO, *Intercettazioni di comunicazioni*, in AA. VV., *Una nuova legge contro la corruzione. Commento alla legge 9 gennaio 2019, n. 3*, a cura di R. Orlandi-S. Seminara, Giappichelli, 2019, p. 245 ss.; G. TABASCO, *Intercettazioni, a mezzo di captatore informatico, nei procedimenti per i delitti contro la pubblica amministrazione*, in AA. VV., *La legge anticorruzione 9 gennaio 2019, n. 3*. Aggiornata alla l. 28 giugno 2019, a cura di M. Del Tufo, Giappichelli, 2019, p. 153 ss.; M. TORRE, Il *captatore informatico dopo la legge c.d. spazza-corrotti,* in *Dir. pen. proc*., 2019, f. 5, p. 651.

[200] Si esprime così M. TORRE, *Il captatore informatico dopo la legge c.d. spazza-corrotti*, cit., p. 651.

[201] Restano, dunque, esclusi i reati commessi da incaricati di pubblico servizio o da esercenti servizi di pubblica necessità, nonché quelli commessi da privati nei confronti della pubblica amministrazione.

[202] Per espressa previsione normativa, la preventiva individuazione, anche indiretta, dei «luoghi e del tempo», in relazione ai quali è consentita l'attivazione della spia elettronica da remoto, è circoscritta

Va, tuttavia, rilevato che la norma così formulata risulta alquanto ambigua e nebulosa.

Più in particolare, il contrato esegetico deriva dall'inciso «e per i delitti dei pubblici ufficiali contro la pubblica amministrazione […]», inserito dopo le parole «se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3 *bis* e 3 *quater* c.p.p.».

Parte della dottrina, soffermandosi sul dato letterale della disposizione, ritiene di dover mantenere ferma la disciplina derogatoria all'autorizzazione rafforzata solo nel caso in cui si proceda per la cerchia dei reati elencati dall'art. 51, commi 3 *bis* e 3 *quater* c.p.p.; viceversa, relazione ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione, il decreto deve indicare i luoghi e i tempo in relazione ai quali è consentita l'attivazione del captatore informatico[203].

Come evidenziato, tuttavia, per evitare di incorrere in un'interpretazione illogica e contraddittoria, si ritiene più opportuno ricorrere ad «un'interpretazione terapeutica»[204] di tipo sistematico che faccia leva sulla *ratio* della novella. Conseguentemente l'art. 267 c.p.p. deve essere letto alla luce delle modifiche apportate all'art. 266, comma 2 *bis* c.p.p.: se attualmente, per i reati dei pubblici ufficiali contro la pubblica amministrazione, l'intercettazione tra presenti nei luoghi domiciliari è consentita indipendentemente dalla dimostrazione che tali luoghi siano sede di attività criminosa in atto, ne discende che non è più necessario, per i medesimi reati, individuare e indicare preventivamente il contesto spazio-temporale da monitorare.

Lo stesso vale, *a fortiori*, per i luoghi diversi da quelli di cui all'art. 614 c.p., all'interno dei quali l'esigenza di tutelare la sfera di intimità e riservatezza degli interlocutori *ivi* presenti risulta certamente affievolita.

Al di là delle discutibili scelte di politica criminale e legislativa effettuate dal legislatore contemporaneo, allo stato dell'arte permangono difficoltà interpretative legate alla disciplina da applicare alle investigazioni inerenti a procedimenti per reati contro la pubblica amministrazione dopo l'entrata il vigore della legge[205]. Ci si trova di fronte ad una "*vacatio legis*" del tutto anomala: la legge è stata promulgata ed è, di fatto, entrata in vigore nel gennaio 2019, tuttavia, la modifica interviene su una norma – l'art. 266, comma 2 *bis* – che, per converso, non è vigente. Di conseguenza, deve ritenersi che, pur essendo già stata approvata, l'effettiva efficacia di tale disposizione è di fatto prorogata al 30 aprile 2020.

---

ai casi in cui si procede per delitti «diversi» da quelli di criminalità organizzata e terrorismo (art. 51, commi 3 *bis* e 3 *quater*, c.p.p.). La legge la legge "anticorruzione" intende accostare, anche sotto il profilo dell'onere motivazionale, i delitti corruttivi a quelli di criminalità organizzata e terrorismo, prevedendo, per entrambe le categorie delittuose, un'eccezione alla regola della doverosa predeterminazione del dato spazio-temporale, con riferimento a cui è consentita l'attivazione del microfono del captatore informatico.

[203] Cfr. M. TORRE, *Il captatore informatico dopo la legge c.d. spazza-corrotti,* cit., p. 651.

[204] L'espressione appartiene a M. TORRE, *Il captatore informatico dopo la legge c.d. spazza-corrotti*, cit., p. 651. Segue una simile prospettiva L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico,* cit., p. 9.

[205] Sul punto, si consenta il rinvio a Cap. III, § 3.1.

7. LA "RIFORMA DELLA RIFORMA FANTASMA": DAL D.L. 161/2019 ALLA L. 7/2020

Troppo superficialmente si è pensato che la *querelle* sorta in merito all'impiego del captatore informatico nel processo penale potesse aver trovato soddisfazione con la riforma del 2017, raffinata nel 2019.

L'effetto domino scaturito dai prodotti legislativi che hanno posposto l'operatività del d.lgs. 216/2017, chiaro sintomo del malcontento della nuova maggioranza governativa, incita il governo ad intervenire, questa volta in maniera definitiva.

Così, proprio il 31 dicembre 2019, nel giorno della sua entrata in vigore[206], il Consiglio dei Ministri, con una manovra repentina, modifica la disciplina *ivi* contenuta[207].

La novella del 2019 incide profondamente sulla normativa prefigurata nel 2017, in relazione alla quale l'esigenza di riservatezza sembra aver ceduto il passo all'efficientamento delle indagini: l'impiego dello strumento, infatti, viene esteso anche ai provvedimenti relativi a categorie delittuose ulteriori e l'utilizzo dei risultati da esso scaturenti viene consentito anche per la prova di reati diversi da quelli per cui è stato emesso il decreto autorizzativo.

---

[206] Come anticipato, l'entrata in vigore della c.d. "riforma Orlando" era prevista per il 31 dicembre 2019, a seguito dell'ennesima proroga operata dal "Decreto Sicurezza-*bis*".

[207] D.l. 30 dicembre 2019, n. 161, recante "*Disposizioni urgenti in materia di intercettazioni*", in *Gazz. uff*., 31 dicembre 2019, n. 305. Per i primi commenti si vedano L. FILIPPI, *D.l. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, in *Il quotidiano giuridico*, 10 gennaio 2020; ID., *Intercettazioni:* habemus legem!, in *Dir. pen. proc*., 2020, f. 4, p. 453 ss.; M. GRIFFO, *Il* Trojan *e le derive del terzo binario. Dalla riforma Orlando al d.l. 161/2019, passando per la "spazzacorrotti" e il decreto sicurezza* bis, in *Sist. pen*., 2020, f. 2, p. 61 ss.; ID., *Rilievi sull'impiego del* trojan *nei procedimenti per i reati contro la pubblica amministrazione*, in *Proc. pen. giust*., 2020, n. 2, p. 482 ss.; W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, *ivi,* 2020, f. 1, p. 63 ss.; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, *ivi*, 2020, f. 1, p. 109 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni, ivi,* 2020, f. 2, p. 71 ss.; G. SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni, ivi*, 2020, f. 1, p. 47 ss.: A. SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *Arch. pen*., 2020, f. 1, p. 1. Il 31 dicembre 2019 è stato assegnato alla Commissione giustizia in sede referente il disegno di legge ordinaria, intitolato: "*Conversione in legge del decreto-legge 30 dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*", presentato dal Presidente del Consiglio dei Ministri Conte e dall'*ex* Ministro della Giustizia Bonafede. Il 20 febbraio 2020, il Senato approva, con modificazioni rispetto al testo proponente, il disegno di legge d'iniziativa del Governo. Cfr. Disegno di legge n. 1659, avente ad oggetto "*Conversione in legge, con modificazioni, del d.l. 30 dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni e comunicazioni*", in *www.senato.it*. Il d.l. n. 161/2019 viene poi convertito, con modificazioni, dalla l. 28 febbraio 2020, n. 7, in *Gazz. uff*. 28 febbraio 2020, n. 50. Per i primi commenti, v. O. CALAVITA, *Intercettazioni: sul captatore informatico rimangono alcune perplessità*, in *Ist. dir. econ.,* 2020, f. 1, p. 152 ss.; C. PARODI, *Convertito il d.l. 161/2019 in materia di intercettazioni: le correzioni di rotta,* in *www.ilPenalista.it,* 26 febbraio 2020; D. PRETTI, *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019*, in *www.sistemapenale.it,* 2 marzo 2020; G. SPANGHER, *Dl intercettazioni: una controriforma dall'avvio incerto*, in *Guida dir.,* 2020, n. 10, p. 14; ID., *La riforma sconta due mesi di proroga, in vigore dal 1° maggio*, *ivi*, 2020, n. 13, p. 34; ID., *La (contro)riforma delle intercettazioni telefoniche*, in *Studium Iuris*, 2020, f. 5, p. 529 ss.

Benchè al nuovo legislatore sia stata concessa la *chance* di "correggere il tiro" rispetto agli errori fatti e rilevati dalla dottrina e dalla giurisprudenza durante quest'ultimo biennio, la riforma sembra acuire le preoccupazioni degli esperti del settore, nascondendo molte insidie per la tenuta del sistema e l'efficacia stessa dello strumento intercettivo[208].

Al fine di individuare gli elementi di novità apportati dal legislatore del 2020, occorre inevitabilmente richiamare l'impianto normativo su cui si sedimenta la novella.

Come già anticipato, il d.lgs. n. 216/2017 ha introdotto un nuovo comma 2 *bis* all'art. 266 c.p.p., prevedendo che sono sempre consentite le intercettazioni tra presenti – anche nei luoghi di privata dimora (art. 614 c.p.), a prescindere dalla sussistenza del fondato motivo di ritenere che in quel luogo si stia svolgendo un'attività criminosa – mediante l'inserimento di captatore informatico solo nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater,* c.p.p.[209]; viceversa, per tutte le altre fattispecie delittuose, le captazioni mediante *virus* informatico in ambito domiciliare possono essere autorizzate solo ove sussista il sopra indicato requisito, seguendo la regolare disciplina delle intercettazioni[210].

Su questo impianto è poi intervenuta la l. n. 3/2019 che, innestando nella disposizione di cui all'art. 266, comma 2 *bis,* c.p.p. una nuova categoria criminosa, equipara i procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione, puniti con la reclusione non inferiore nel limite massimo a cinque anni, a quelli di cui agli artt. 51, commi 3 *bis* e 3 *quater* c.p.p.[211].

Tali modifiche, mai divenute operative perché inserite nel corpo di disposizioni non entrate in vigore, sono oggetto di ulteriore interpolazione ad opera del d.l. n. 161/2019 con la specificazione che i delitti contro la pubblica amministrazione per cui si applica la disciplina di cui all'art. 266, comma 2 *bis,* c.p.p., sono quelli commessi, oltre che dai pubblici ufficiali, anche dagli incaricati di pubblico servizio[212].

---

[208] In questo senso W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, cit., p. 63 ss.; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità, cit.,* p. 109 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 71 ss.

[209] L'innesto è avvenuto ad opera dell'art. 4, comma 1, lett. *a,* punto 2 d.lgs. n. 216/2017.

[210] Sul tema, diffusamente, T. ALESCI, *Le intrusioni* inter praesentes, cit., p. 77.

[211] Art. 1, comma 4, lett. *a,* l. n. 3/2019. Più precisamente, il comma 3 della medesima novella abroga il secondo comma dell'art. 6, d.lgs. n. 216/2017, il quale stabiliva che «[L]l'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 del codice penale non può essere eseguita mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile quando non vi è fondato motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa».

[212] Art. 2, comma 1, lett. *f,* punto 1, d.l. n. 161/2019. Come noto, *ex* art. 357 c.p., sono considerati pubblici ufficiali «coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi»; sono, invece, incaricati di pubblico servizio *ex* art. 358 c.p., «coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale». Dunque, a titolo esemplificativo, è considerato pubblico ufficiale, l'insegnante, l'ufficiale giudiziario, l'ufficiale sanitario; è, invece, incaricato di pubblico servizio, una guardia giurata, un idraulico o un operaio del comune, il controllore dell'autobus o del treno. Sul

Come precisato, questa interpolazione sembra rivolta ad affrontare uno dei dubbi interpretativi che gli art. 4 e 6 del d.lgs. n. 216 del 2017 poteva ingenerare[213]. L'estensione dell'area operativa del captatore informatico, infatti, era stata delimitata da queste norme con riferimento ai «procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni».

Una interpretazione letterale di tali disposizioni poteva indurre a ritenere che gli *standard* richiesti per le indagini in tema di criminalità organizzata fossero stati estesi alle investigazioni che, nell'ambito dei delitti contro la pubblica amministrazione, riguardavano più precisamente quelli di cui al Capo I - intitolato proprio "*Dei delitti dei pubblici ufficiali contro la pubblica amministrazione*" - del Titolo II del Libro II c.p.[214].

La previsione in parola, ai fini del ricorso al captatore informatico nei reati contro la pubblica amministrazione, riconosce rilievo alla qualifica soggettiva riconosciuta all'indagato: come precistao, «[S]sembra sostenibile, pertanto, che lo strumento tecnologico in esame possa essere impiegato per tutti i "delitti contro la pubblica amministrazione", compresi nel titolo II, del Libro II del codice penale, commessi tanto dai pubblici ufficiali, quanto dagli incaricati di pubblico servizio, ovviamente sempre che sussistano i presupposti di ammissibilità indicati dalla norma […]»[215].

Allo stato dell'arte, dunque, vige una disciplina "tripartita" in materia di captazioni nei luoghi domiciliari mediante *Trojan*: da una parte, vi sono i reati di criminalità organizzata ed economica (richiamati dall'art. 266, comma 2 *bis* c.p.p.), per cui sono sempre consentite le intercettazioni ambientali domiciliari; dall'altra, i reati "comuni", per i quali, invece, l'impiego dello strumento soggiace ai limiti di cui al comma 2 del medesimo articolo; dall'altra ancora, esiste una normazione ibrida in relazione ai procedimenti facenti capo a un'associazione per delinquere seppur diversa dalle fattispecie contemplate dall'art. 51, commi 3 *bis* e 3 *quater* c.p.p.[216] - nonché quelli la cui disciplina risulta

---

tema, da ultimo, M. LOMBARDO, *Le qualifiche soggettive*, in AA. VV., *Delitti dei pubblici ufficiali contro la pubblica amministrazione*, a cura di A. Marandola-B. Romano, Utet, 2020, p. 28 ss. Come osservato, «si tratta di una modifica più di forma che di sostanza, nel senso che, implementando le categorie di soggetti per cui il captatore informatico può trovare legittimamente impiego, il legislatore ne amplia indirettamente la portata anche ai reati ascrivibili in capo agli incaricati di pubblico servizio». W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, cit., p. 69. In effetti, nel diritto penale le qualifiche di pubblico ufficiale e di incaricato di pubblico servizio rilevano per la configurabilità di determinati reati commessi da o contro tali soggetti. In sostanza, la differente qualifica rileva affinché un reato possa dirsi integrato. Si pensi, ad esempio, al reato di "*Concussione*" (art. 317 c.p.) o al delitto di "*Corruzione per l'esercizio della funzione*" (art. 318 c.p.), ovvero al reato di "*Corruzione per un atto contrario ai doveri d'ufficio*" (art. 319 c.p.) che si qualificano come reati commessi esclusivamente dal pubblico ufficiale e al reato di "*Corruzione di persona incaricata di un pubblico servizio*" (art. 320 c.p.), commesso, invece, solo dall'incaricato di pubblico servizio. Sul tema, esaustivamente, L. FILIPPI, *Le intercettazioni*, in AA. VV., *Delitti dei pubblici ufficiali contro la pubblica amministrazione*, cit., p. 557 ss.

[213] Relazione dell'Ufficio del Massimario della Corte di Cassazione, cit., p. 8 s.

[214] Si tratta dei reati compresi tra gli artt. 314 e 335 *bis* c.p., i quali, peraltro, sono delitti che possono essere commessi sia da pubblici ufficiali, sia da incaricati di pubblico servizio, con esclusione di alcune fattispecie penali, come, ad esempio, la turbata libertà degli incanti (art. 353 c.p.) e la turbata libertà del procedimento di scelta del contraente (art. 353 *bis* c.p.).

[215] *Relazione dell'Ufficio del Massimario della Corte di Cassazione*, cit., 8.

[216] Si tratta, più precisamente, dei procedimenti facenti capo ad un'associazione per delinquere, *ex* art. 416 c.p., correlate alle attività criminose più diverse, con esclusione del mero concorso di

equiparata all'art. 13 del d.l. n. 152/91 - per i quali, invece, pur non essendo previsto un limite all'intrusione domiciliare in ragione del "doppio binario investigativo", non trova applicazione né la disciplina più estensiva del nuovo comma 2 *bis* dell'art. 266 c.p.p. né le altre disposizioni derogatorie di cui all'art. 267, comma 1 e 2 *bis,* c.p.p.

In relazione al decreto autorizzativo "rafforzato", il comma 1 dell'art. 267 c.p.p. viene progressivamente arricchito, prima dall'art. 4, comma 1, lett. *b*, punto 1 del d.lgs. n. 216/2017 che introduce la precisazione dei tempi e dei luoghi oggetto di captazione nel caso in cui si proceda per delitti diversi da quelli di cui all'art. 51, commi 3 *bis* e 3 *quater,* c.p.p.; poi l'art. 1, comma 4, lett*. b),* l. n. 3/2019, che amplia la deroga ai delitti commessi dai pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni determinata ai sensi dell'art. 4 c.p.p. Da ultimo, l'art. 2, comma 1, lett. *d),* punto 1, d.l. n. 161/2019 prevede che la deroga valga anche nel caso degli stessi delitti commessi dagli incaricati di pubblico servizio.

Occorre solo un'ultima precisazione: come espressamente previsto in sede di conversione del d.l. n. 161/2019, nel caso in cui si proceda per delitti contro la pubblica amministrazione di cui all'art. 266, comma 2 *bis,* c.p.p., il decreto autorizzativo dovrà anche specificare le ragioni che giustificano l'impiego del captatore informatico e l'esercizio delle operazioni anche nei luoghi di cui all'art. 614 c.p.[217].

Tale contenuto non sembra coincidere con il fondato motivo per ritenere che in un ambiente, riconducibile alla previsione dell'art. 614 c.p., sia in corso l'attività criminosa, presupposto richiesto dall'art. 266, comma 2 c.p.p. per lo svolgimento di intercettazioni tra presenti per reati diversi da quelli contemplati dal comma 2 *bis* dello stesso articolo in simili luoghi. Si tratta, verosimilmente, «di qualcosa di meno della dimostrazione che sia in atto l'attività criminosa, ma comunque di un dato che vale a giustificare l'intrusione nel domicilio»[218].

Così facendo, il legislatore intende diversificare ulteriormente la disciplina prevista per i reati economici rispetto a quella riservata ai reati di cui all'art. 51, commi 3 *bis* e 3 *quater,* c.p.p., aggravando gli oneri motivazionali del giudice.

In sostanza, il decreto autorizzativo, pur non dovendo indicare i luoghi e i tempi delle captazioni in ragione del disposto di cui all'art. 267, comma 1, c.p.p., deve, per converso, prevedere i motivi che giustificano il ricorso allo strumento per le captazioni domiciliari che, è bene ribadirlo, non soggiace ad alcuna limitazione, secondo il disposto di cui all'art. 266, comma 2 *bis,* c.p.p.

Discutibile appare la scelta di aggravare l'onere motivazione da parte del giudicante allorquando autorizza il compimento delle operazioni di intercettazione mediante captatore informatico all'interno del domicilio qualora si proceda per reati contro la pubblica amministrazione[219].

Come osservato, l'"utilità" richiesta «appare difficilmente rinnegabile, posto che […] anche facilmente intuibile l'utilità di una intercettazione all'interno dell'abitazione,

---

persone nel reato, per cui si applicano le disposizioni di cui all'art. 13, d.l. n. 152/91 in forza di quanto indicato da Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[217] Cfr. art. 1, comma 1, l. n. 7/2020, che modifica l'art. 2, comma 1, lett. *c* del d.l. n. 161/2019.

[218] *Relazione dell'Ufficio del Massimario della Corte di Cassazione,* cit., p. 10.

[219] Sul tema, diffusamente, ID., *Rilievi sull'impiego del* trojan *nei procedimenti per i reati contro la pubblica amministrazione*, cit., p. 482 ss.

specialmente laddove si ipotizzino confidenze dell'indagato con i familiari conviventi. Se si considera poi che, non trattandosi di un presupposto di ammissibilità, l'eventuale omessa indicazione delle suddette ragioni non sconta certamente la sanzione di inutilizzabilità dei risultati, di cui al comma 1 dell'art. 271 c.p.p., in quanto non eseguita al di fuori dei casi consentiti dalla legge, la novità appare, francamente, di modesta portata innovativa»[220].

In relazione, invece, ai profili "tecnici", vanno segnalate, le modifiche apportate all'art. 89 disp. att. c.p.p. Si interviene sul comma 2, prevedendo che, ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili devono – anziché possono – essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministero della giustizia. Si tratta di una modifica che, nel voler rafforzare il divieto d'uso di programmi non conformi, appare di scarso impatto rispetto a quanto già era previsto dal "decreto Bonafede".

Al comma 3 del medesimo articolo, viene introdotta una nuova procedura di trasferimento e custodia dei dati appresi, per cui gli stessi devono essere "conferiti" presso gli impianti della procura della Repubblica[221] e *ivi* trasmessi ricorrendo a procedute tecniche idonee a garantire l'integrale corrispondenza tra quanto registrato e trasmesso[222]. Se, tuttavia, appare impossibile procedere al contestuale trasferimento dei dati intercettati, il verbale dovrà anche indicare le ragioni tecniche impeditive e della successione cronologica degli accadimenti captati e delle conversazioni intercettate.

L'aspetto maggiormente rilevante della novella del 2020 inerisce alle riforme che intaccano la disciplina dei divieti di utilizzazione probatoria dei dati illegittimamente appresi (art. 270 c.p.p.)[223].

---

[220] Così D. PRETTI, *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019*, cit., p. 8.

[221] Secondo l'art. 2, comma 2, lett. *a*, d.l. n. 161/2019, le comunicazioni intercettate dovevano essere trasferite esclusivamente nell'archivio digitale di cui all'art. 269, comma 1, c.p.p.; diposizione, poi, modificata in sede di conversione. Come osservato, «l'intercettazione continuerà, anche nella vigenza delle nuove disposizioni, ad essere effettuata attraverso gli impianti, pur installati pur presso le sale *server* degli uffici requirenti, appartenenti alle società di intercettazione accreditate o aggiudicatarie del servizio e, soltanto ad operazioni ultimate, avverrà il trasferimento dei dati da tali *server* a quello, ministeriale, dell'archivio digitale». D. PRETTI, *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019,* cit., p. 7 s.

[222] Art. 2, comma 2, lett. *a)*, d.l. n. 161/2019.

[223] Invero, l'utilizzabilità dei risultati delle intercettazioni in procedimenti diversi è un tema "caldo" nel panorama giuridico dottrinale e giurisprudenziale. Di recente, la S.C., nella sua composizione più autorevole, interviene per chiarire la portata del dettato di cui all'art. 270, comma 1, c.p.p. In quell'occasione, la Corte chiarisce che il divieto in esame non opera, oltre che nel caso di reati successivamente emersi che siano ricompresi tra quelli per cui è previsto l'arresto obbligatorio in flagranza, anche con riferimento ai risultati relativi ai reati che sono connessi *ex* art. 12 c.p.p., sempre che rientrino nei limiti di ammissibilità previsti dalla legge. Cass., sez. un., 28 novembre 2019, n. 51, in *Proc. pen. giust*. Sul tema, G. ILLUMINATI, *Utilizzazione delle intercettazioni in procedimenti diversi: le sezioni unite ristabiliscono la legalità costituzionale*, in *www.sistemapenale.it*, 30 gennaio 2020. Sul punto anche G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., p. 143 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 102 ss.

Più precisamente, il comma 1 dell'art. 270 c.p.p., rimasto immune ai ritocchi normativi pregressi[224], subisce una modifica in sede di conversione sotto un duplice profilo[225]: da un lato, si rafforzano le condizioni che legittimano l'impiego dei risultati captativi in procedimenti diversi da quelli indicati nel decreto autorizzativo; dall'altro, viene introdotta un'ulteriore ipotesi derogatoria al regime di inutilizzabilità, prevedendo che la trasmigrazione del captato possa considerarsi legittima allorquando risulti «necessaria e indispensabile» non solo per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio, ma anche dei reati di cui all'art. 266, comma 1 c.p.p.[226].

L'inserimento, a distanza di meno di due mesi dalla pronuncia delle Sezioni unite "Cavallo"[227], del riferimento all'art. 266 c.p.p. potrebbe indurre a ritenere, in sede di prima ma poco attenta esegesi della norma, che il legislatore abbia inteso positivizzare le condizioni indicate dalla Suprema Corte ai fini dell'impiego extraprocedimentale delle risultanze intercettive, laddove è stato stabilito che l'utilizzabilità delle captazioni in procedimenti diversi, in quanto connessi ai sensi dell'art. 12 c.p.p. rispetto ai reati per cui l'autorizzazione era stata originariamente concessa, richiede in ogni caso che si tratti di reati ricompresi nel catalogo declinato dall'art. 266 c.p.p., ovverosia di reati per i quali sarebbero comunque state consentite *ab origine* le operazioni di intercettazione.

Come anche sostenuto dalla dottrina[228], una simile lettura non può essere avallata, in quanto il riferimento all'art. 266 c.p.p. nell'attuale formulazione dell'art. 270 c.p.p. è accostato non all'indicazione del divieto di utilizzazione in procedimenti diversi

---

[224] Come precisa F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, in *Sist. pen*., 2020, f. 5, p. 233, «[I]il primo comma della richiamata disposizione […] era sopravvissuto indenne, nella versione licenziata dai codificatori del 1988, anche all'impeto riformatore del legislatore del 2017 […]».

[225] Le ragioni dell'intervento sul primo comma della disposizione non emergono con chiarezza dai lavori parlamentari: la Relazione che accompagnava la presentazione al Senato del d.l. 161/20167, in vista della conversione, si limitava ad affermare che «in ordine all'articolo 270 si interviene attraverso la modifica dei riferimenti normativi relativi al procedimento di stralcio, al fine di coordinare la norma con le modifiche all'articolo 268, e con una rimodulazione, anche alla luce della recentissima sentenza delle sezioni unite della Corte di cassazione, della norma limitativa delle possibilità di utilizzazione dei risultati delle intercettazioni captate tramite *trojan* per la prova di reati diversi da quelli in relazione ai quali l'intercettazione era stata autorizzata». Così Così *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019*, cit. Nei lavori di Commissione, l'immediato antecedente all'emendamento che avrebbe, infine, riscritto il testo del primo comma dell'art. 270 c.p.p. nella versione definitiva – ed attualmente vigente – si rintraccia nell'emendamento 2.86 a firma dell'On. Grasso, che, in accordo al *dictum* delle Sezioni unite "Cavallo", prevedeva la riscrittura del primo comma, nei termini che seguono «i risultati delle intercettazioni non possono essere utilizzati per la prova di reati diversi da quelli nei quali sono stati disposti, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza o per i reati che risultino connessi ai sensi dell'articolo 12 del codice di procedura penale». Tale emendamento viene ritirato dallo stesso proponente e, su iniziativa del Relatore, è sostituito dall'emendamento 2.2191, che propone l'integrale riscrittura del primo comma dell'art. 270 c.p.p., così come poi approvato sia dal Senato che dalla Camera.

[226] L. n. 7/2020, che modifica l'art. 2, comma 1, lett. *g)*, d.l. n. 161/2019, attraverso l'interpolazione di un nuovo punto "01". Per un primo commento, A. MARANDOLA, *Intercettazioni: una riforma nel segno della "non dispersione". I nuovi limiti di utilizzabilità* ex *art. 270 c.p.p.,* in *www.ilPenalista.it.,* 24 febbraio 2020.

[227] Cass., sez. un., 28 novembre 2019, n. 51, cit.

[228] In questo senso, D. PRETTI, *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019*, cit., p. 10.

quanto piuttosto alle ipotesi dei reati per i quali sia previsto l'arresto obbligatorio in flagranza e per i quali l'utilizzabilità è invece ammessa senza limiti.

Di conseguenza, la nuova disciplina ammette l'impiego dei risultati delle intercettazioni in procedimenti diversi non soltanto qualora le captazioni risultino necessarie ed indispensabili per l'accertamento dei delitti per i quali sia previsto l'arresto obbligatorio in flagranza ma anche, in alternativa, per i reati indicati nel corpo del comma 1 dell'art. 266 c.p.p. E la bontà di tale soluzione interpretativa trova conferma, peraltro, proprio nei lavori parlamentari[229] laddove si indica che tale modifica *estende* l'utilizzabilità delle intercettazioni in procedimenti diversi anche nei casi indicati dall'art. 266 c.p.p. per i quali non sia previsto l'arresto obbligatorio in flagranza[230].

Per quanto concerne il comma 1 *bis* dell'art. 270 c.p.p., nella formulazione originaria del 2017, si era previsto che i risultati raccolti mediante captatore informatico non potessero essere utilizzati per la prova di delitti diversi da quelli autorizzati, «salvo che gli stessi siano necessari per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio».

Sul punto, il legislatore del 2020 interviene in maniera assai incisiva, ribaltando la struttura della disposizione che, da norma di divieto, si trasforma in una norma di autorizzazione, con l'unica condizione che i reati da provare rientrino nella categoria di quelli per i quali il ricorso al captatore è autorizzato dal relativo decreto.

Ai sensi della nuova normativa, fermo restando il divieto di impiego del prodotto delle captazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte[231], «[…] i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2 *bis*» c.p.p.[232], condizionando il loro impiego al canone della "indispensabilità"[233].

Allo stato, dunque, è possibile utilizzare le risultanze delle attività captative condotte mediante *Trojan* per la prova di reati diversi da quelli contemplati dal decreto autorizzativo, purchè ricompresi tra i gravi crimini di cui all'art. 51, commi 3 *bis* e 3 *quater,* c.p.p. e quelli commessi dai pubblici ufficiali o gli incaricati di pubblico servizio contro la pubblica amministrazione, nonché per la prova dei delitti per i quali è obbligatorio l'arresto in flagranza.

A ben guardare, la contro-riforma tende a sgretolare la regola dell'inutilizzabilità, estendendo il perimetro di operatività del regime derogatorio: nell'ottica di un

---

[229] Cfr. il parere della Commissione permanente Affari Costituzionali del Senato della Repubblica del 19 febbraio 2020 relativamente all'emendamento n. 2.219. In questo senso anche *Relazione dell'Ufficio del Massimario della Corte di Cassazione*, cit., p. 13.

[230] Per dovere di completezza, si precisa che in sede di conversione del d.l. n. 161/2019, viene introdotto una nuova fattispecie nel catalogo dei reati intercettabili *ex* art. 266, comma 1, c.p.p., rappresentata dai «delitti commessi avvalendosi delle condizioni previste dall'art. 416 *bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste nello stesso articolo» (art. 266, comma 1, lett. *f quinquies),* c.p.p.).

[231] *Ex* art. 270, comma 1, c.p.p.

[232] Cfr. art. 2, comma 1, lett. *g*, punto 1, d.l. n. 161/2019.

[233] L. n. 7/2020, che modifica l'art. 2, comma 1, lett. *g,* d.l. n. 161/2019.

coordinamento con l'interpretazione fornita dalla Suprema Corte al concetto di "diverso reato" e "diverso procedimento"[234], si deve ritenere che il divieto di circolazione delle informazioni apprese mediante captatore non opera (oltre che in relazione ai casi espressamente previsti dal dettato normativo di cui al comma 1 dell'art. 270 c.p.p., espressamente richiamato nell'incipit del comma 1 *bis* del medesimo articolo), con riferimento ai reati diversi ma connessi *ex* art. 12 c.p.p.[235], nonché ai reati diversi non connessi che rientrano nei casi di cui all'art. 266, comma 2 *bis* c.p.p.[236].

La novella apre, dunque, la strada "libera" circolazione probatoria delle risultanze della captazione digitale determinando una sostanziale violazione della garanzia della riserva di giurisdizione prevista dall'art. 15 Cost.[237], con riferimento all'intercettazione confluita nel "procedimento diverso", in assenza di qualsivoglia controllo da parte del giudice procedente.

In sostanza, il rischio è che una volta ottenuta l'autorizzazione all'impiego del *virus* informatico in riferimento ad un certo reato all'interno di un determinato procedimento – e quindi anche sulla base di motivi concernenti la posizione dell'indagato in quel procedimento per quella specifica fattispecie delittuosa – le informazioni ottenute possano essere utilizzate anche in indagini diverse per la prova di reati differenti, benché, in questi non sussistano o comunque non siano stati verificati i presupposti per l'emissione di un analogo provvedimento autorizzativo[238].

---

[234] Cass., sez. un., 28 novembre 2019, n. 51, cit.

[235] Per cui, è bene precisarlo nuovamente, non opera il divieto di cui all'art. 270, comma 1, c.p.p., non trattandosi di "reati diversi". Cfr. Cass., sez. un., 28 novembre 2019, n. 51, cit.

[236] Sul punto, efficacemente, G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, Delibera CSM, *Parere sul disegno di legge 1659 AS di conversione del d.l. 161/2019*, cit., p. 5.

[237] Sul punto, esaustivamente, A. CAMON, *Le intercettazioni telefoniche nel processo penale*, Giuffrè, Milano, 1996, p. 44. Più di recente e con riferimento alla normativa modificata nel 2017, P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 255 ss.

[238] P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 262; ID., *L'impiego del* trojan horse *informatico nelle indagini penali*, cit., p. 329 ss.

CAPITOLO II

IL LATO OSCURO DELLE RIFORME: IL CAPTATORE INFORMATICO OLTRE I CONFINI DELLE INTERCETTAZIONI

SOMMARIO: 1. Il tentativo di tipizzazione delle operazioni mediante captatore: un inedito congegno per le categorie tradizionali del diritto – 2. Il *malware* quale mezzo di esecuzione delle intercettazioni ambientali: un'angusta categoria probatoria – 2.1. *Segue*: la cimice informatica per le intercettazioni telefoniche e telematiche – 3. Le altre funzioni: ispezioni, perquisizioni e sequestri informatici tramite *Trojan* – 4. L'acquisizione dei dati informatici tra sequestro di corrispondenza e intercettazione telematica – 4.1 *Segue*: l'acquisizione dei dati custoditi nel *Cloud* – 5. Le attività investigative mediante captatore nel *genus* delle prove atipiche – 6. Le perquisizioni *online* – 6.1 *Segue*: il pedinamento "informatico" tramite *Trojan*– 6.2 *Segue*: lo *screenshot* e il *keylogging* – 6.3. *Segue*: le videoriprese investigative – 7. Il captatore informatico tra atipicità, irritualità e incostituzionalità

1. IL TENTATIVO DI TIPIZZAZIONE DELLE OPERAZIONI MEDIANTE CAPTATORE: UN INEDITO CONGEGNO PER LE CATEGORIE TRADIZIONALI DEL DIRITTO

È materia molto delicata quella delle nuove investigazioni eseguite mediante captatore informatico che, al di là del già intricato tema delle intercettazioni, s'ingarbuglia pericolosamente per le potenzialità dirompenti che il *malware* può generare, per i conseguenti attentati mossi ai tradizionali paradigmi del procedimento probatorio e, più di tutto, per la "confusione" giuridica in cui versa questa speciale tecnica investigativa nel sistema processuale italiano.

In questo quadro magmatico, in cui ogni tentativo di analisi sconta un perdonabile margine di errore e una probabile non condivisione, il legislatore cerca la soluzione più agevole, quella che comporta meno sacrificio in termini di utilità investigativa senza rinunciare – almeno formalmente – alla tutela dei diritti inviolabili, scegliendo di delimitare le funzionalità del *virus* informatico alla sola captazione delle registrazioni audio, attraverso l'attivazione del microfono del dispositivo infetto[1].

L'obiettivo è quello di attribuire al captatore un preciso volto, quello di una «cimice informatica»[2], ossia uno strumento inedito per dare esecuzione ad un mezzo tradizionale di ricerca della prova, rappresentato dall'intercettazione di conversazioni e comunicazioni tra presenti (art. 266, comma 2 c.p.p.)[3].

---

[1] Come sapientemente osservato, «[L]la deriva autoritaria delle prassi e l'abuso degli strumenti investigativi, soprattutto quelli non tipizzati, attraverso il ricorso alla analogia, è perspicuamente ricavabile dalla comparsa sugli scenari investigativi del captatore informatico». Così M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, Editoriale Scientifica, 2019, p. 97.

[2] Lo definiscono in tal modo D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in AA. VV., *Le recenti riforme in materia penale*, a cura di G.M. Baccari-C. Bonzano-K. La Regina- E.M. Mancuso, Wolters Kluwer-Cedam, 2017, p. 560.

[3] Parla di un'intercettazione atipica priva di una sua autonomia concettuale, S. LORUSSO, Digital evidence, cybercrime *e giustizia penale 2.0*, in *Proc. pen. giust.,* 2019, f. 4, p. 823.

Una simile volontà traspare nitidamente dai criteri direttivi contenuti nella legge delega[4] ma anche dal successivo decreto attuativo[5] e dagli spasmodici interventi riformatori[6].

Tuttavia, troppo superficialmente si è pensato che la scelta (non sovvertita né ampliata dal legislatore della contro-riforma) di limitare la funzionalità del captatore fosse condivisibile, sul rilievo che, attraverso la sola attivazione del microfono del dispositivo elettronico portatile su cui il *malware* viene inoculato, si sarebbero superate le resistenze di chi aveva visto nello strumento una creatura «bulimica»[7] capace di condurre, nello stesso momento, plurime attività. Sul punto, infatti, la dottrina avanza delle riserve[8], ritenendo che «il lato "nascosto", su cui la novella è rimasta silente, crea difficoltà interpretative ancor maggiori di quelle direttamente legate alla lettura del testo»[9].

In effetti, la mancanza di una precisa regolamentazione della materia crea un vuoto di tutela che contrappone chi propende per l'illiceità della "altre" attività che il *virus* –

---

[4] Cfr. art. 1, comma 84, lett. *e*, n. 1 della l. 23 giugno 2017, n. 103, recante "*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*", in *Gazz. uff.,* 4 luglio 2017, n. 154, per cui «l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto»; nonché nell' art. 1, comma 84, lett. *e*, n. 2, della medesima novella, il quale si riferisce espressamente alla «registrazione audio» che deve essere avviata dalla polizia giudiziaria.

[5] Il d.lgs. 29 dicembre 2017, n. 216, recante "*Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017,* n. 103", in *Gazz. uff.,* 11 gennaio 2018, n. 8, procede alla modifica del solo art. 266, comma 2 c.p.p. al fine di prevedere una nuova modalità di esecuzione delle intercettazioni tra presenti mediante l'inserimento di un captatore informatico inoculato su dispositivi elettronici portatili.

[6] A ben guardare, né la l. 9 gennaio 2019, n. 3, recante "*Misure per il contrasto dei reati contro la pubblica amministrazione, nonchè in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*", in *Gazz. uff*., 16 gennaio 2019, n. 13, né la l. 28 febbraio 2020, n. 7, avente ad oggetto "*Conversione in legge, con modificazioni, del decreto-legge 30 dicembre 2019, n. 161, recante modifiche urgenti alla disciplina delle intercettazioni di conversazioni o comunicazioni*", in *Gazz. uff*., 28 febbraio 2020, n. 50.7/2020 apportano alcuna modifica all'impianto predisposto dal legislatore precedente in relazione all'inquadramento giuridico dell'attività condotta tramite *Trojan*.

[7] Così L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, in *Arch. pen*., 2016, f. 2, p. 350.

[8] *Ex multis*, P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in AA. VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra-R. Orlandi, Giappichelli, 2018, p. 237 s.; O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, in *Dir. pen. cont*., 2018, f. 11, p. 51 s.; D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 561 ss.; F. RUGGIERI, *L'impatto delle nuove tecnologie: il captatore informatico. L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, in *Jusonline*, 2017, f. 3, p. 357; G. SPANGHER, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giur. pen.* web, n. 1, 2018; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, in *Sist. pen*., 2020, n. 2, p. 150, per cui l'impostazione è «minimalista e riduttiva».

[9] L'espressione appartiene a L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, in AA. VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 290.

almeno in potenza – è in grado di dispiegare[10] e chi, al contrario, ne ammette una qualche forma di utilizzo in ragione della "tipicità" dei risultati probatori ottenuti[11].

Stante l'incidenza sul piano dei diritti fondamentali di una simile tecnica investigativa, secondo alcuni Autori parrebbe necessario limitarne il più possibile la sfera operativa, restringendo il campo di azione alle sole intercettazioni di comunicazioni tra presenti, come espressamente previsto dal legislatore: la mancanza di una previsione legislativa espressa delle funzioni diverse dalla captazione di conversazioni e comunicazioni *ex* art. 266, comma 2 c.p.p., «potrebbe suonare come un'esclusione»[12].

Contrariamente, si sostiene che la lacuna legislativa non permette di ritenere che le attività investigative di cui si discute debbano ritenersi vietate e, come tali, insuscettibili di fornire materiali probatori utilizzabili in giudizio (art. 191 c.p.p.). Ciò «perché alcune di tali attività […] sono riconducibili a strumenti di ricerca della prova già disciplinati dalla legge (segnatamente, l'intercettazione di comunicazioni) e comunque, perché nel sistema processuale penale italiano non esiste un principio di tassatività della prova, essendo il giudice espressamente autorizzato ad assumere anche "prove non disciplinate dalla legge" (art. 189 c.p.p.)»[13].

Di qui, nonostante l'introduzione di una legge *ad hoc* volta a disciplinare l'impiego del captatore informatico nel processo penale quale strumento tecnico di intercettazione[14],

---

[10] Seguono una simile interpretazione, R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, f. 2, p. 538 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 299 ss.; M. TROGU, *Intrusioni segrete nel domicilio informatico*, in AA. VV., *Le indagini atipiche*, a cura di A. Scalfati, II ed., 2019, p. 579.

[11]Seguendo l'interpretazione di F. CORDERO, *Tre studi sulle prove,* Giuffrè, 1963, p. 153, per cui «tutto ciò che non è vietato dalla legge è permesso», parte della dottrina sostiene che le altre attività siano utilizzabili nei limiti delle regole di cui all'art. 189 c.p.p. Cfr. P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in. *Riv. it. sc. giur*., 2017, f. 8, p. 347 s.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* in *Rev. brasileira dir. proc. pen*., Porto Alegre, 2017, vol. 3, f. 2, p. 485 ss.

[12] Si esprime così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 301. Nello stesso senso R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 544 s., il quale precisa che «[U]usi diversi da quelli espressamente regolati dall'art. 266, comma 2 e comma 2 *bis* c.p.p. non sono ammessi, proprio perché limitano un diritto fondamentale di una persona […], del quale è però doveroso affermare l'esistenza […]».

[13] In questo senso F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* cit., p. 485 ss.

[14] Il *malware* viene definito in tal modo da M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *Dir. pen. cont*., 20 dicembre 2018. Si veda anche l'impostazione di O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, 2005, p. 25, che così definisce la «componente» dello «strumento di prova», il cui intervento «nell'impiego dei mezzi di prova è per alcuni loro esemplari necessario e per altri eventuale»: «essa consiste in apparati conoscitivi (principi e metodologie della scienza teorica, metodiche della scienza applicata, tecnologie, procedure di indagini tecniche e di valutazioni costruite sulla scorta di esperienze pratiche specializzate, apparecchiature con cui queste risorse di conoscenza sono utilizzate) che esorbitano dal sapere comune quanto a competenza teorica o pratica e richiedono perciò il ricorso a un esperto». Proprio al novero delle «apparecchiature tecniche» appare riconducibile il captatore informatico, quale «componente ulteriore rispetto a quelle individuate nelle previsioni del catalogo» codicistico.

il sofisticato arnese tecnologico continua a suscitare un indubbio disagio nell'interprete, spiegabile con la congenita illimitatezza delle sue potenzialità.

Abituato a ragionare per ambiti e categorie giuridiche entro i quali imbrigliare potestà e diritti, il giurista si sente disarmato dinanzi ad un mezzo, non solo duttile rispetto a plurime attività di indagine, sia tipiche che atipiche, ma anche in grado di svolgerle cumulativamente senza limiti spazio-temporali. Conseguentemente, scartata l'interpretazione più ovvia di classificare il congegno come autonomo mezzo di ricerca della prova, se ne propone l'artificiosa partizione sulla base di un criterio funzionale, teso a ricondurre ciascuna delle poliedriche attività consentite dal *software* sotto l'egida del mezzo probatorio più affine, al fine di verificare, per ciascuna funzione, l'esistenza o meno di una copertura normativa[15].

In sostanza, a ciascuna categoria "tecnica" si tenterà di ascrivere un contenuto giuridico, ossia specifiche attività di indagine le quali, nel loro insieme, delineano la multifunzionalità del *software Trojan.*

La questione sulla compatibilità delle attività *de quibus* rispetto agli strumenti tipici (o atipici) non rappresenta una velleità teoretica, in quanto dalla risoluzione dell'enigma discende la legittimità dei risultati ottenuti dall'impiego del captatore, oltre la funzione di cimice informatica.

2. IL *MALWARE* QUALE MEZZO DI ESECUZIONE DELLE INTERCETTAZIONI AMBIENTALI: UN'ANGUSTA CATEGORIA PROBATORIA

La prima categoria probatoria con cui sembra opportuno confrontarsi è rappresentata dall'istituto delle intercettazioni di conversazioni e comunicazioni tra presenti (art. 266, comma 2 c.p.p.), in ragione della sussunzione legislativa delle operazioni di captazione mediante *virus Trojan* nell'ambito di tale mezzo di ricerca della prova tipico.

Ai fini dell'indagine, occorre *in primis* soffermarsi sulla complessa nozione di "intercettazione", in modo da evidenziare gli elementi che contribuiscono ad assimilare o, al contrario, a differenziare l'attività di captazione derivante dall'accensione del microfono del dispositivo "infettato" da quelle esperibile mediante le tradizionali tecniche intercettive.

Il preliminare tentativo di definizione del concetto di intercettazione non è il frutto di un mero esercizio dogmatico ma è espressione di un ineludibile bisogno per chi, chiamato ad applicare la relativa disciplina, si trova a fronteggiare la necessità di distinguere attività

[15] Lo costatano G. BARROCU, *Il captatore informatico. Un* virus *per tutte le stagioni*, in *Dir. pen. proc*., 2017, f. 3, p. 379 ss.; A. CAMON, *Cavalli di Troia in Cassazione,* in *Arch. nuova proc. pen*., 2017, f. 1, p. 79; L. CUOMO-L. GIORDANO, *Informatica e processo penale*, in *Proc. pen. giust*., 2017, f. 4, p. 729 s.; A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite* virus *informatico,* in AA. VV., *Le indagini atipiche*, II ed., cit., p. 607 ss.; M. TORRE, *Sistemi informatici di controllo e riservatezza. Una proposta di regolamentazione del captatore informatico*, in *www.ilpenalista.it*, 2017. Viceversa, rifiuta la costruzione parcellizzata del captatore per classificarlo alla stregua di una «nuova e diversa tipologia di mezzo di prova», L. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen*. online, p. 1 ss.

investigative differenti eppure tra loro molto simili, ad alcune delle quali solamente è riferibile la normativa in materia di intercettazione[16].

Come noto, all'interno del codice di rito non è contenuta alcuna definizione di "intercettazione"[17] ma la lacuna viene colmata per via giurisprudenziale che, valorizzando le informazioni fornite dalla dottrina[18], definisce l'attività *de qua* quale «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere gli altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato»[19].

---

[16] In questo senso E. APRILE, *Intercettazioni di comunicazioni*, in AA. VV., *Prove,* a cura di A. Scalfati, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, 2009, p. 475 s.

[17] Sottolineano l'assenza di una definizione legislativa del concetto di intercettazione, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 476; A. BARGI–S. FURFARO, *Le intercettazioni di conversazioni e comunicazioni*, in AA. VV., *La prova penale*, a cura di A. Gaito, Giappichelli, 2008, p. 113 s.; L. FILIPPI, *Intercettazione,* in AA. VV., *La prova penale*, a cura di P. Ferrua–E. Marzadura–G. Spangher, Giappichelli, 2013, p. 837; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007; D. SIRACUSANO–F. SIRACUSANO, *Le prove,* in AA. VV., *Diritto processuale penale*, a cura di G. Di Chiara–V. Patanè–F. Siracusano, Giuffrè, 2018, p. 318 s.

[18] La dottrina dominante definiva l'intercettazione, ancor prima del dirimente intervento giurisprudenziale chiarificatore (su cui vedi nt. 19), come «la presa di conoscenza, operata clandestinamente da un terzo con l'impiego di mezzi meccanici o elettronici di captazione del suono, delle comunicazioni segrete attuate in forma diversa dallo scritto». Così A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996 p. 12. Contribuiscono a fornire una nozione di intercettazione E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche*, Giuffrè, 2004, p. 2 s.; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. disc. pen*., VII, Utet, 2001, p. 178; F. CAPRIOLI, *Intercettazione e registrazione di colloqui tra persone presenti nel passaggio dal vecchio al nuovo codice di procedura penale*, in *Riv. it. dir. proc. pen*., 1991, f. 1, p. 155; L. FILIPPI, voce *Intercettazioni telefoniche (diritto processuale penale),* in *Enc. dir*., VI, Giuffrè, 2002, p. 565; ID., *L'intercettazione di comunicazioni*, Giuffrè, 1997, p. 33 ss.; C. FRANCHINI, voce *Intercettazione di comunicazioni*, in *Enc. giur*., Treccani, 1988, p. 1 ss.; G. FUMU, sub *artt. 266–271*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, 1990, II ed., p. 774; S. FURFARO, voce *Intercettazioni (profili di riforma),* in *Dig. disc. pen.,* X, Utet, 2018; L. GRANATA, *Le intercettazioni telefoniche nel nostro codice di procedura penale*, in *Riv. polizia*, 1961, p. 449 ss.; V. GREVI, *Appunti in tema di intercettazioni telefoniche operate dalla polizia,* in *Riv. it. dir. proc. pen*., 1967, f. 3, p. 724 ss.; P. GROSSO, voce *Intercettazioni telefoniche*, in *Enc. dir.,* XXI, Giuffrè, 1971, p. 889 s.; C. PARODI, *Le intercettazioni. Profili operativi giurisprudenziali,* Giappichelli, 2002, p. 88 ss.; G. SPANGHER, *La disciplina italiana delle intercettazioni di conversazioni o comunicazioni*, in *Arch. pen*., 1994, f. 1, p. 77 ss. Durante la vigenza del Codice del 1930, G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Giuffrè, 1983, p. 171 ss. Sottolineano la specificità della "primitiva" definizione dottrinale, più di recente, M. BRANCACCIO, sub *art. 266,* in *Codice di procedura penale,* a cura di G. Canzio–R. Bricchetti, Milano, 2017, p. 1987 ss.; L. FILIPPI, sub *art. 266*, in *Codice di procedura penale commentato*, a cura di A. Giarda–G. Spangher, Milano, 2017, V ed., p. 2547 ss.

[19] Cfr. Cass., sez un., 28 maggio 2003, n. 36747, in *Guida dir*., 2003, f. 42, p. 55 ss. Per commenti sulla rivoluzionaria pronuncia, L. FILIPPI, *Le Sezioni Unite decretano la morte dell'agente segreto "attrezzato per il suono"*, in *Cass. pen.,* 2004, f. 10, p. 2094 ss.; G. FUMU, *Registrazione di colloqui tra presenti effettuata a cura della polizia giudiziaria: insuperabili i limiti alla testimonianza indiretta*, in *Riv. polizia*, 2003, f. 11, p. 762 ss.; E. ROSCIANO, *Dalla registrazione clandestina dei colloqui tra polizia giudiziaria e confidenti all'ambito applicativo degli "altri casi" di cui all'art. 195 c.p.p.,* in *Giust. pen.,* 2004, f. 12, p. 682 ss. Già prima della citata pronuncia i giudici di legittimità avevano tentato di fornire una definizione compiuta dell'istituto. Cfr. Cass., sez. un., 23 febbraio 2000, n. 6, in *Cass. pen*., 2000, f. 1, p. 255 ss. Si veda anche Corte cost., 6 aprile 1993, n. 81, in *Giur. cost*., 1993, p. 731 ss.

Da quanto detto, emerge che, per poter annoverare una mera ricezione di dati e informazioni nel concetto ben più ampio e articolato di "intercettazione"[20], sono richieste alcune caratteristiche inequivocabili dell'atto intercettivo, in quanto «non ogni forma di captazione di dialoghi o conversazioni rientra nel *genus* in esame»[21].

Perché ciò si verifichi devono sussistere i seguenti requisiti: occorre che i soggetti comunichino tra loro con il preciso intento di escludere gli altri dal contenuto della comunicazione e in modo tale da tenere quest'ultima segreta; è necessario l'uso di strumenti tecnici di percezione particolarmente invasivi e tali da superare le cautele elementari che dovrebbero garantire la libertà e la segretezza del colloquio ed a captarne i contenuti; infine, il soggetto captante deve essere assolutamente estraneo al colloquio, violando – in modo "clandestino" – la segretezza della conversazione[22].

In relazione all'oggetto delle intercettazioni, il codice di rito inerisce alle comunicazioni e alle conversazioni: come precisato dalla dottrina, «si tratta di concetti aventi un'estensione […] concentrica, laddove le conversazioni rappresentano una forma di comunicazione perché relativa allo scambio di dati informativi che si attua mediante l'uso della voce»[23].

Detto in altri termini, tale mezzo di ricerca della prova mira all'apprensione di flussi di conversazioni e comunicazioni espletabile attraverso le differenti tipologie di intercettazioni telefoniche (art. 266, comma 1 c.p.p.), ambientali e domiciliari (art. 266, comma 2 c.p.p.) e telematiche (art. 266 *bis* c.p.p.).

---

[20] È opportuno distinguere nettamente le intercettazioni dalle altre attività "collaterali" che, pur consistendo nell'apprensione di flussi comunicativi, non possono essere ricomprese nell'ambito degli artt. 266 ss. c.p.p. La giurisprudenza sul tema è assai ampia. Solo a titolo esemplificativo, non costituisce intercettazione: l'acquisizione di messaggi registrati nella segreteria telefonica (Cass., sez. VI, 8 gennaio 2002, n. 3940, in *Guida dir.*, 2002, f. 3, p. 86 ss.); l'acquisizione dei dati segnalati sul *display* del telefono cellulare (Cass., sez. IV, 29 gennaio 2004, n. 3435, in *Cass. pen*., 2006, p. 536); le conversazioni o comunicazioni attuate con l'uso di emittenti a irradiazione circolare (Cass., sez. I, 20 maggio 1997, n. 5894, in *CED Cass*., n. 207931); la registrazione di conversazioni effettuata ad opera della p.g. con persona informate sui fatti (Cass., sez. II, 24 febbraio 2010, n. 1695, in *Guida dir*., 2010, f. 15, p. 88 ss.).

[21] Si esprime così P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, cit., p. 178.

[22] Sui caratteri dell'atto intercettivo, senza pretese di completezza, si rinvia a A. BARGI, *Sulla distinzione tra "registrazione" di un colloquio ad opera di uno dei partecipanti ed "intercettazione" di una conversazione da parte di estranei*, in *Cass. pen.,* 1982, f. 10, p. 2028 ss.; A. BARGI–S. FURFARO, *Le intercettazioni di conversazioni e di comunicazioni,* cit., p. 113 s.; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, cit., p. 179 s.; A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 19 s.; L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 6 s.; P. GROSSO, voce *Intercettazioni telefoniche*, cit., p. 890; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 33 s.; A. PACE, *Problematica delle libertà costituzionali,* Cedam, 1992, p. 241 s.; G. SABATINI, voce *Prova (dir. proc. pen.),* in *Noviss. dig. it*., XIV, Utet, 1967, p. 332; D. SIRACUSANO, *Le prove*, in AA. VV., *Manuale di diritto processuale penale*, a cura di A. Galati–D. Siracusano–G. Tranchina–V. Zappalà, Giuffrè, 1990, p. 450 Più di recente, A. BALSAMO, *Intercettazioni: gli* standards *europei, la realtà italiana, le prospettive di riforma,* in *Cass. pen*., 2009, f. 12, p. 4023 ss.; F. CAPRIOLI, *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime,* in AA. VV., *Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti,* Atti del Convegno, 5–7 ottobre 2007, Giuffrè, 2007, p. 146 ss.; C. PARODI, *Le intercettazioni. Profili operativi giurisprudenziali,* cit., p. 88 ss.; G. SPANGHER, *Le criticità della disciplina delle intercettazioni telefoniche,* in *Dir. pen. proc.*, 2016, f. 8, p. 921 ss.; ID., *Linee guida per una riforma delle intercettazioni telefoniche, ivi,* 2008, f. 10, p. 1209 ss.

[23] Così E. APRILE, *Intercettazioni di comunicazioni,* cit., p. 476.

A fronte delle inevitabili limitazioni alle più basiche libertà fondamentali (artt. 14 e 15 Cost.), il legislatore, pur non fornendo alcuna definizione alle operazioni *de qua*, introduce un regime giuridico assai preciso e dettagliato, precisando i "casi" di

intercettazione[24], i presupposti per procedere all'esecuzione delle operazioni[25], l'*iter* autorizzativo[26] e i termini di durata[27].

[24] Nelle intercettazioni tradizionali il catalogo di reati per cui l'attività investigativa risulta legittima sembra assai ampio e variegato, potendosi esperire captazioni processuali per tutte le fattispecie di cui all'art. 266, comma 1 c.p.p. ovvero, nel caso di intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266 *bis* c.p.p., anche per i reati commessi mediante l'impiego di tecnologie informatiche o telematiche. In particolare, il legislatore individua i reati per cui sono consentite le intercettazioni prevalentemente sulla base di un criterio di natura quantitativa, incentrato sull'entità della pena edittale, determinata a norma dell'art. 4 c.p.p. Si tratta dei delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni, ovvero per i delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni. In altri casi, il legislatore utilizza un criterio qualitativo, indicando i reati–tipo per cui è esperibile il mezzo di ricerca della prova (delitti concernenti sostanze stupefacenti o psicotrope; quelli concernenti le armi e le sostanze esplosive; delitti di contrabbando; reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, molestie; divulgazione di materiale pedopornografico e adescamento di minorenni; *stalking.* Da ultimo, la l. 7/2020 estende i casi di intercettazione anche ai «delitti commessi avvalendosi delle condizioni previste dall'art. 416 *bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste nello stesso articolo»). Sul tema, esaustivamente, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 479 ss.; A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 64; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale*, Giappichelli, 2016, p. 172 ss.; L. FILIPPI, sub *art. 266,* cit., p. 2571 s.; G. ILLUMINATI, *La disciplina processuale delle intercettazioni,* cit., p. 74 s.; S. FURFARO, voce *Intercettazioni (profili di riforma),* cit., già pubblicato in *Arch. pen*., f. 1, 2018; E. MARZADURI, *Spunti per una riflessione sui presupposti applicativi delle intercettazioni telefoniche a fini probatori*, in *Cass. pen*., 2008, f. 11, p. 4833 ss.; L. SIMEONE, *I reati associativi,* Maggioli editore, 2015, p. 53 ss.

[25] Ai sensi dell'art. 267 c.p.p., le intercettazioni vengono autorizzate solo se risultano «assolutamente indispensabili ai fini della prosecuzione delle indagini», qualora sussistano «gravi indizi di reato». Per i reati di criminalità organizzata e terrorismo, la norma prevede dei requisiti "attenuati" rispetto a quelli tradizionali: le intercettazioni tra presenti possono essere condotte anche nel domicilio a prescindere dal "fondato motivo di ritenere che in quel luogo si stia consumando un'attività criminosa"; l'intercettazione è ammessa sulla basi di "sufficienti indizi" (e non gravi, *ex* art. 267 c.p.p.), quando la stessa è "necessaria" (e non indispensabile *ex* art. 267 c.p.p.) alla prosecuzione delle indagini. Cfr. art. 13, d.l. 13 maggio 1991, n. 152, recante "*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*", in *Gazz. uff.,* 13 maggio 1991, n. 110, convertito, con modificazioni, in l. 12 luglio 1991, n. 203, in *Gazz, uff.*, 12 luglio 1991, n. 162. In tema, anche in chiave critica, F. ALONZI, *La Costituzione impone rigore nell'interpretare i presupposti applicativi delle intercettazioni telefoniche*, in *Arch. pen.* online, p. 1*;* P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni,* cit., p. 189; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale*, cit., p. 199 ss.; G. CONSO, *Intercettazioni telefoniche: troppe e troppo facilmente divulgabili,* in *Dir. pen. proc*., 1996, f. 1, p. 137 ss.; M.L. DI BITONTO, *Lungo la strada per la riforma della disciplina delle intercettazioni*, in *Cass. pen.,* 2008, f. 1, p. 18 ss.; L. FILIPPI, sub *art. 267*, cit., p. 2622 ss.; ID., *L'intercettazione di comunicazioni e il segreto di polizia*, in AA. VV., *Giusto processo. Nuove norme sulla formazione e valutazione della prova (l. 1.3.2001 n. 63),* a cura di P. Tonini, Cedam, 2001, p. 387 ss.; ID., *L'intercettazione di comunicazioni,* cit., p. 72 s.; G. GIOSTRA, *Intercettazioni tra indagini e* privacy, in *Dir. e giust*., 2006, f. 31, p. 98 s.; V. GREVI, *Le intercettazioni come mero "mezzo di ricerca" di riscontri probatori?*, in *Cass. pen*., 2009, f. 6, p. 848 ss.; G. ILLUMINATI, *La disciplina processuale delle intercettazioni,* cit., p. 81 s.; G. SPANGHER, *Linee guida per una riforma delle intercettazioni telefoniche,* in *Dir. pen. proc*., 2008, f. 9, p. 1209 s. Per una ricostruzione della speciale disciplina derogatoria, da ultimo, M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 22 ss.

[26] Nelle intercettazioni l'autorizzazione è fornita dal giudice per le indagini preliminari, il quale decide sulla richiesta del p.m. con decreto motivato non impugnabile. Nei casi d'urgenza, quando «vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini» il p.m. dispone l'intercettazione con decreto motivato che va comunicato immediatamente (e, comunque, non oltre le ventiquattro ore) al g.i.p. il quale, entro quarantotto ore, decide sulla convalida con

Tratteggiate in questo modo le caratteristiche dell'istituto, si è detto che «[N]non c'è dubbio che in questa generica fattispecie possano rientrare anche le captazioni effettuate per il tramite del dispositivo elettronico informaticamente modificato»[28], sul rilievo che la materia è stata regolamentata in un momento storico nel quale le potenzialità intrusive degli strumenti di captazione risultavano assai minori di quelle che possono oggi vantare uno *smartphone* o un *tablet* controllati a distanza. Di conseguenza, anche le attività *de quibus* rientrerebbero a pieno titolo nel *genus* delle intercettazioni, non rilevando che le nuove tecniche investigative risultino oggetto di una precisa regolamentazione normativa sul presupposto che la bontà dell'assetto normativo espresso dagli artt. 266 ss. c.p.p. prescinda dal tipo di tecnologia di volta in volta impiegata[29].

Secondo altra parte di dottrina, la possibilità di inquadrare l'attività in esame nell'ambito del mezzo tipico di ricerca della prova non risulta così scontata, potendo reggere solo «a patto che oggetto della captazione sia effettivamente una comunicazione e non anche dati [non comunicativi] già presenti e memorizzati all'interno dei dispositivi informatici»[30].

Nulla quaestio, dunque, se l'attività intercettativa tramite agenti intrusori fosse circoscritta alla captazione di un flusso comunicativo intercorrente tra due o più soggetti. E, in effetti, il legislatore sembra rispettare tale "sillogismo": proprio al fine di equiparare le intercettazioni tramite captatore a quelle tradizionali, circoscrive le potenzialità dello strumento alla sola apprensione di comunicazioni e conversazioni attraverso la mera attivazione del microfono del dispositivo sul quale il *malware* agisce.

In questi termini, l'esito della ricerca suonerebbe tranquillizzante sul piano della legalità: perimetro e modalità operative sono dettata tassativamente dal codice e

---

decreto motivato (art. 267 c.p.p.). Sul tema, *amplius*, P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, cit., p. 188 s.; A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 79 ss.; L. FILIPPI, sub *art. 267*, in *Codice di procedura penale commentato*, V ed., cit., p. 2628. Come sapientemente rilevato, «il decreto autorizzativo si atteggia rispetto alle intercettazioni telefoniche alla medesima stregua delle condizioni di procedibilità in riferimento all'esercizio dell'azione penale». Così A. GAITO, *Limiti all'utilizzabilità delle intercettazioni telefoniche nelle decisioni sulla libertà personale*, in *Giur. it.,* 1992, f. 2, p. 513. Nello stesso senso, V. CAMPILONGO, *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi*, in *Cass. pen*., 2005, f. 11, p. 3196 ss. Da ultimo, A. FIASCHI, *L'uso della motivazione* "per relationem" *nei decreti autorizzativi delle intercettazioni*, in *Dir. pen. proc.,* 2018, f. 1, p. 100 ss.; E. PILLA, *Provvedimenti e motivazione*, in AA. VV., *L'intercettazione di comunicazioni*, cit., p. 117. Per dovere di completezza, si segnala che la Corte europea dei diritti dell'uomo ha disposto che non costituisce violazione dell'art. 8 CEDU l'autorizzazione all'esecuzione di intercettazioni ambientali disposta mediante un provvedimento motivato *per relationem*. Cfr. Corte EDU, sez. II, 10 aprile 2007, *Panarisi c. Italia*, n. 4679/99. Sul punto, v. A. BALSAMO, *Intercettazioni: gli* standards *europei, la realtà italiana, le prospettive di riforma*, cit., p. 4023 ss.

[27] Ai sensi dell'art. 267, comma 3 c.p.p., la durata delle intercettazioni processuali «non può superare i quindici giorni, prorogabili per periodi successivi di quindici. In relazione ai delitti di criminalità organizzata, invece, il termine massimo è di quaranta giorni, prorogabili di venti, ai sensi dell'art. 13, d.l. 13 maggio 1991, n. 152, cit. Per tutti, L. FILIPPI, sub *art. 267*, cit., p. 2643 ss.

[28] F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* cit., p. 494. Nello stesso senso anche A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite* virus *informatico,* cit. p. 606 s.

[29] Sul tema G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "tra presenti*", in *Dir. pen. cont*., 7 ottobre 2016, p. 11.

[30] Si esprime così M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017, p. 25 s.

subordinate dal provvedimento del giudice, cui è affidato il controllo del canone della stretta necessità dell'incidenza dell'atto intercettivo rispetto ai diritti fondamentali[31].

Va, tuttavia, rilevato che anche una siffatta soluzione sconta un eccessivo semplicismo che finisce per nascondere molte insidie per la tenuta del sistema e l'efficacia stessa dello strumento captativo.

Pur volendo assimilare tali forme captative alle intercettazioni "classiche", non si può negare che le prime siano caratterizzate da «significative peculiarità»[32], risultando molto più intrusive nella vita privata di chi vi è sottoposto e, al contempo, assai più efficaci per i loro esiti istruttori.

In relazione alla maggiore incisività delle nuove tecniche intercettive, si converrà che un conto è posizionare microspie in un determinato luogo ("ambiente") oggetto di intercettazione, altro è inoculare un *virus Trojan* all'interno di un dispositivo elettronico portatile, per cui l'interpolazione tra l'utente e l'universo *web* consente di accedere all'intera rete dei rapporti sociali e affettivi che nascono e si sviluppano nel cyberspazio. Come rilevato, il telefono cellulare è, oramai, «uno strumento che accompagna ogni movimento del soggetto» ed è ovvio che, se usato con finalità captatorie, è in grado di operare un controllo indiscriminato della vita privata e sociale di ogni individuo[33].

Saltano, a questo punto, le categorie di riferimento: qualora l'attività di captazione segua tutti gli
spostamenti del possessore del *mobile device*, diventa privo di significato discorrere, come fa l'art. 266, comma 2 c.p.p., di una determinata categoria di soggetti presenti. Il *virus* informatico estende il proprio raggio di azione «alla folla indeterminata e indeterminabile di persone, [anche estranee ai fatti di indagine], che in qualunque luogo conversano»[34] e, allargato ed infittito il «"*secret garden*" delle relazioni interpersonali»[35], cresce in misura speculare il *vulnus* inferto alla dignità umana dalla violazione dei suoi confini.

Di qui, deve dubitarsi che tali attività possano essere agevolmente sussunte nella disciplina di cui agli artt. 266 c.p.p. che, come anticipato, «consente limitazioni "mirate" a determinati luoghi o persona»[36], circoscrivendo l'ambito della captazione in modo ben preciso.

Ciò è imposto dall'art. 15, comma 1 Cost. che, proclamando l'"inviolabilità" delle comunicazioni e riservando la possibilità di limitarle al previo «atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge», pone la "doppia garanzia" della riserva di legge e di giurisdizione proprio al fine di circoscrivere soggettivamente ed

---

[31] Come precisato dalla giurisprudenza, per poter essere ritenuta legittima, dunque, la compressione deve essere «proporzionata rispetto alla giustificazione invocata al fine di non oltrepassare i limiti della stretta necessità». Così Corte EDU, sez. III, 14 marzo 2002, *Puzinas c. Lituania*, n. 44800/98; Corte EDU, sez. I, 9 gennaio 2001, *Natoli c. Italia,* n. 26161/95, § 33; Corte EDU, 23 settembre 1998, *McLeod c. Regno Unito*, 24755/94, § 53.

[32] In questo senso L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit. p. 308.

[33] Così Procura generale presso la Corte di cassazione Memoria per la camera di consiglio delle Sezioni Unite del 28 aprile 2016, in *Quest. giust.,* 4 maggio 2016.

[34] A. CAPONE, *Intercettazioni e costituzione*. *Problemi vecchi e nuovi*, in *Cass. pen*., 2017, f. 3, p. 1263.

[35] A. SANNA, L'irriducibile atipicità delle intercettazioni tramite virus informatico, cit., p. 607.

[36] Così L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, cit., p. 349.

oggettivamente la possibilità di captare le comunicazioni, cioè nei confronti di soggetti determinati e modalità, tempi e luoghi e determinati[37].

Si aggiunga che la giurisprudenza della Corte europea dei diritti dell'uomo introduce dei limiti precisi all'uso delle intercettazioni, prevedendo che il legislatore nazionale abbia il dovere di definire l'ambito di applicazione delle operazioni captative, in modo da dare ai cittadini un'adeguata indicazione delle circostanze in presenza delle quali la pubblica autorità ha il potere di disporle, non solo per quanto attiene alla natura dei reati, ma pure in riferimento ai potenziali destinatari delle captazioni[38].

Come evidenziato, invece, «[S]secondo la nuova tecnologia del captatore "itinerante", nulla è prevedibile dall'ignaro cittadino: infatti, è "determinato" soltanto il dispositivo intercettato in "qualsiasi" luogo si trovi, nelle mani di "chiunque" lo detenga, con "qualunque" persona questi conversi o comunichi, di "qualsiasi" argomento parli o "qualunque" cosa faccia»[39].

In relazione alla maggiore efficacia investigativa degli strumenti tecnici di captazione – direttamente proporzionale alla elevata sua intrusività – può ritenersi che anche quando tramite il *virus* informatico vengono realizzate intercettazioni tra presenti, tali attività si inseriscono in un universo investigativo molto più ampio e complesso, rispetto al quale risulta difficile discernere le ipotesi che possano, senza esitazione, venire assimilate al noto mezzo di ricerca della prova e quelle che, invece, ne devono rimanere distinte. A ben vedere, infatti, gli strumenti tecnici di captazione consentono agli investigatori di acquisire una quantità di dati assai più cospicua rispetto a quella che si realizzerebbe attraverso l'impiego delle tradizionali microspie, avendo, in questo caso, il vantaggio che la captazione non risulta né legata ad un ambiente specifico da monitorare né alla "mera"

---

[37] Sul significato della doppia riserva, v. nt. 189 e 190. Per una disamina del *dictum* di cui all'art. 15 Cost., si consenta il rinvio a Cap. IV.

[38] In effetti, la giurisprudenza della Corte di Strasburgo è assai attenta ad individuare le regole per determinare la compatibilità dell'istituto delle intercettazioni rispetto al precetto di cui all'art. 8 CEDU. Emblematica, in questo senso, è la recente sentenza della Così Corte EDU, Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, n. 47143/15, § 227. In quell'occasione i Giudici di Strasburgo hanno ritenuto che «la legge russa non rispetta il criterio sulla "qualità della legge" e che è incapace di limitare l'intercettazione di comunicazioni a quanto "necessario in una società democratica"», con conseguente violazione dell'articolo 8 della Convenzione. In tema A. BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea,* in *Cass. pen.,* 2016, p. 2278 ss.; S. BASILICO–E. MARIANI, *Monitoraggio Corte Edu dicembre 2015*, a cura di G. Ubertis–F. Viganò, in *Dir. pen. cont.*, 15 marzo 2016. Si veda, inoltre, Corte EDU, sez. I, 23 febbraio 2016, *Capriotti c. Italia*, cit. Nello stesso senso, Corte EDU, sez. IV, 12 gennaio 2016, *Szabò e Vissy c. Ungheria*, n. 37138/14. Ma già Corte EDU, sez. IV, 10 febbraio 2009, *Iordachi c. Moldavia*, n. 25198/02, in *Cass. pen*., f. 10, 4029 ss. In dottrina, su ciascuno dei requisiti, E. APRILE, *Diritto processuale penale europeo e internazionale*, Cedam, 2007, p. 202 ss.; A. BALSAMO, *Intercettazioni: gli* standars *europei, la realtà italiana e le prospettive di riforma,* cit., p. 4023 ss.; A. DIDDI, *L'inviolabilità della segretezza delle comunicazioni*, in AA. VV., *Processo penale e costituzione*, a cura di F.R. Dinacci, Giuffrè, 2010, p. 274 ss.; S. FURFARO, *Un problema irrisolto: le intercettazioni telefoniche*, in AA. VV., *Procedura penale e garanzie europee,* a cura di A. Gaito, Utet, 2006, p. 117; A. GAITO-S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza,* in AA. VV., I *principi europei del processo penale*, a cura di A. Gaito, p. 363 ss.; A. TAMIETTI, *Le intercettazioni tra garanzie fondamentali e sostanziali,* in AA. VV., *Giurisprudenza europea e processo penale italiano*, a cura di A. Balsamo–R.E. Kostoris, Giappichelli, 2008, p. 426 ss.; G. UBERTIS, *Principi di procedura penale europea. Le regole sul giusto processo*, Giuffrè, 2000, p. 105 ss.

[39] L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, cit., p. 351.

apprensione di conversazioni e comunicazioni, conferendo all'attività in esame maggiore flessibilità ed efficacia.

Gli effetti sugli esiti processuali non sono di poco conto: potendo carpire anche tutto quanto esula dal concetto di "conversazione e comunicazione" – ossia anche suoni e rumori, nonché parole pronunciate da persone vicine al monitorato[40] – i dati ottenuti possono agevolmente transitare in altri procedimenti, non soggiacendo ai limiti di cui all'art. 270 c.p.p.[41], anche qualora questi dovessero avvenire nei luoghi di privata dimora[42].

Da quanto detto, emerge che, sebbene l'attività assuma apparentemente le sembianze delle tradizionali captazioni tra presenti, la normativa "vecchio stile" solo in parte può risultare adeguata a regolare il fenomeno; di conseguenza, l'istituto delle intercettazioni, risentendo dell'evoluzione tecnico-scientifica degli strumenti di captazione, diventa inadatto a contenere tutte quelle attività di indagine "nuove" o "atipiche" messe a disposizione dalla tecnologia.

Ciò rende necessaria un'attenta rivalutazione normativa delle captazioni mediante *virus* informatico, dal momento che – pur volendo immaginare una limitazione delle funzioni del captatore informatico alla solo attivazione del microfono del dispositivo infettato – difficilmente può essere ricompresa esclusivamente nell'alveo delle intercettazioni di comunicazioni tra presenti, pena la violazione dei principi costituzionali e convenzionali che presidiano un istituto già di per sé «non auspicabile e difficilmente compatibile in una società democratica»[43].

---

[40] Solo per dimostrare l'importanza della captazione di simili informazioni, si pensi al pianto di un bambino percosso, al colpo di una pistola utilizzata per uccidere o ferire, al tonfo dei colpi di un bastone utilizzato per ledere un soggetto, la voce di una persona che parla da sola confessando il delitto o esplicitando la propria innocenza.

[41] Come precisato dalla giurisprudenza di legittimità, «i contenuti di intercettazioni legittimamente autorizzate, sono utilizzabili quale mezzo di prova atipico, non trovando applicazione la disciplina in materia di intercettazioni». Così Cass., sez. un. 23 luglio 2014, n. 32697, in *Dir. pen. proc*., 2014, f. 12, p. 1448, con nota critica di A. INNOCENTI, *Le Sezioni Unite aprono all'utilizzabilità dei risultati di intercettazioni disposte in "diverso procedimento".* In particolare, la Corte delinea una distinzione fondamentale tra intercettazioni di comunicazioni in senso proprio e registrazioni sonore effettuate incidentalmente rispetto all'esecuzione delle prime, prevedendo che queste ultime soggiacciono ai limiti di cui all'art. 189 c.p.p. Di qui, la Corte puntualizza che nel caso di specie la disposizione sulla prova atipica risulta applicabile dato che l'intercettazione era stata compiute in luogo non tutelato dall'art. 14 Cost. Di conseguenza, qualora la captazione dovesse avvenire in luoghi protetti dall'art. 14 Cost., i relativi risultati sarebbero inutilizzabili, essendo raccolti in violazione del divieto costituzionale dell'inviolabilità domiciliare.

[42] La puntualizzazione deriva da un'impostazione dottrinale che rintraccia nei principi generali del diritto processuale penale la ragione per cui i risultati captativi non comunicativi raccolti nel corso dell'esecuzione di intercettazioni legittimamente disposte dall'autorità giudiziaria anche in un luogo di privata dimora possono essere utilizzati. Come precisato, «[L]l'utilizzabilità dei risultati non comunicativi delle intercettazioni è garantita dai principi generali […] del diritto e, segnatamente, da quello […] della naturale utilizzabilità del risultato di una legittima attività di indagine». Si esprime così A. INNOCENTI, *Le Sezioni Unite aprono all'utilizzabilità dei risultati di intercettazioni disposte in "diverso procedimento"*, cit., p. 1456.

[43] Così Corte EDU, Grande Camera, 2 agosto 1984, *Malone c. Regno Unito*, n. 8691/79, § 67, in *Publications of the European Court of Human Rights*, vol. 82, pp. 37 ss.

2.1. *SEGUE*: LA CIMICE INFORMATICA PER LE INTERCETTAZIONI TELEFONICHE E TELEMATICHE

Posto che le captazioni effettuate mediante l'ausilio di un *virus Trojan* in modalità di cimice informatica non possono essere ricondotte (solo) alle intercettazioni di conversazioni e comunicazioni tra presenti (art. 266, comma 2 c.p.p.), l'indagine prosegue analizzando la compatibilità dell'attività derivante dall'accensione del microfono sul dispositivo elettronico infettato rispetto alle altre *species* intercettive, ossia quelle telefoniche (art. 266, comma 1 c.p.p.) e telematiche (art. 266 *bis* c.p.p.).

Preliminarmente, occorre individuare le peculiarità di tali forme tipiche di intercettazione, in modo da verificare la sussumibilità delle captazioni così effettuate nella rispettiva sfera operativa.

La prima *species* intercettiva inerisce all'apprensione di conversazioni e comunicazioni che avvengono per il tramite della tradizionale linea telefonica. Come dimostrano orientamenti giurisprudenziali ormai consolidati[44], queste ultime, a differenza delle intercettazioni ambientali, presuppongono l'esistenza di una specifica apparecchiatura o di un particolare sistema da sottoporre ad intercettazione e, conseguentemente, per ciascuna operazione, devono essere precisati nel decreto autorizzativo i dati di identificazione dell'apparecchio da sottoporre a verifica e controllo.

Le intercettazioni di comunicazioni telematiche[45], invece, hanno ad oggetto un «flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi»[46], ossia

---

[44] Cfr. Cass., sez. II, 20 febbraio 2019, n. 19146, in *C.E.D. Cass.,* n. 275583; sez. V, 6 ottobre 2011, n. 5956, *ivi*, n. 252137; sez. VI, 11 dicembre 2007, n. 15396, *ivi,* n. 239634; sez. I, 30 giugno 1999, n. 4561, *ivi,* n. 214036

[45] Le intercettazioni telematiche sono state introdotte nel codice di rito della legge 23 dicembre 1993, n. 547, recante "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*", in *Gazz. uff*., 30 dicembre 1993, n. 305. In particolare, l'art. 11 della novella introduce l'art. 266 *bis* c.p.p., rubricato *Intercettazioni di comunicazioni informatiche o telematiche*, per cui «[N]nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi». All'indomani della riforma additiva, parte della dottrina contestò l'utilità pratica della disposizione contenuta nell'art. 266 *bis* c.p.p., rilevando come l'art. 266 c.p.p. non limitasse la sua previsione all'intercettazione di conversazioni o comunicazioni telefoniche, ma contenga già un, sia pur generico, riferimento ad "altre forme di telecomunicazioni" (art. 266 comma 1 c.p.p.), sì da consentirne un adattamento automatico ogniqualvolta ulteriori acquisizioni della scienza lo richiedessero. E siccome non può esservi dubbio che le comunicazioni telematiche rientrino nell'ambito delle "altre forme di telecomunicazioni" ecco dimostrata la superfluità della disposizione. Prova ne sia che, anche prima dell'entrata in vigore della l. n. 547 del 1993, nessuno dubitava, ad esempio, della possibilità di intercettare le comunicazioni che avvenivano via fax. Così G. FUMU, sub *art. 266* bis, cit., p. 789 ss. Più di recente, E. APRILE, *Intercettazioni di comunicazioni,* cit., p. 487 s. Sull'argomento, più in generale, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 488 ss.; DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc*., 2013, f. 9, p. 992 ss.; C. PARODI, *La disciplina delle intercettazioni telematiche*, in *Dir. pen. proc*., 2003, f. 8, p. 899; L. FILIPPI, sub art. 266 bis, in Codice di procedura penale commentato, cit., p. 2615 ss.

[46] Il "flusso" può essere definito come il susseguirsi di comunicazioni in corso all'interno di un sistema o tra più sistemi informatici, tra i quali è possibile uno scambio di impulsi che trasmettono informazioni. Per "sistema informatico" deve intendersi qualunque complesso di apparecchiature destinate a compiere qualsiasi funzione utile all'uomo attraverso l'impiego di tecnologie

tra computer collegati tra loro in rete, via modem, via radio (se i dispositivi sono connessi con tecnologia *wireless*) o con qualsiasi altra forma di interconnessione[47].

Tale flusso può essere rappresentato non solo dal tradizionale scambio di *email* o per mezzo delle più svariate applicazioni che consentono l'interazione in tempo reale o differito (servizi di messaggistica e di *chat*)[48] ma anche da *file* sonori e comunicazioni vocali[49] che, come conclamato dalla giurisprudenza di legittimità, «rappresentano a tutti gli effetti un flusso di dati»[50].

---

informatiche. Le comunicazioni tra sistemi informatici – che si concretano in segnali digitali (dati binari o bit) avvengono lungo linee non telefoniche, come quelle impiegate per mettere in collegamento, con l'ausilio di apposite apparecchiature (server), varie postazioni informatiche (Local Area Network). In un sistema telematico, invece, la trasmissione dei dati avviene lungo la linea telefonica, televisiva o satellitare. Sul tema, diffusamente, C. PARODI, *Le intercettazioni. Profili operativi e giurisprudenziali*, Giappichelli, 2002, p. 292 ss. In giurisprudenza, da ultimo, Cass., sez. V, 8 gennaio 2020, n. 4470, in *C.E.D. Cass.*, n. 277885

[47] Sul punto, esaustivamente, L. LUPARIA, *Le investigazioni informatiche nell'ordinamento processuale italiano*, in AA. VV., *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, a cura di L. Luparia-G. Ziccardi, Giuffrè, 2007, p. 162 ss.

[48] Sulla possibilità di compiere intercettazioni telematiche mediante l'ausilio del captatore informatico al fine di acquisire documenti digitali, si rinvia a § ?

[49] In questi casi, l'acquisizione del segnale avviene avvalendosi la c.d. tecnologia *Voip*. Letteralmente l'acronimo sta per "*Voice Over Internet Protocol*". Si tratta di una tecnologia relativamente recente ma che si è ormai fortemente consolidata. La principale funzionalità del *Voip* consiste nella possibilità di effettuare una vera e propria conversazione telefonica sfruttando una preesistente connessione di rete (può trattarsi o di una connessione internet ovvero di un'altra rete all'uopo dedicata che utilizza il protocollo IP) anziché passare attraverso la rete telefonica tradizionale (PSTN- *Public switched telephone network*). La grande particolarità del *Voip* rispetto alle comunicazioni telefoniche tradizionali si rinviene nel fatto che, nell'ambito del suo funzionamento, vengono del tutto eliminate le centrali di commutazione. Il sistema *Voip* infatti, attraverso appositi *software* (chiamati *gateways*), provvede ad instradare sulla rete pacchetti di dati contenenti le "informazioni vocali" (analogiche) codificate e compresse in forma digitale (*bits*), solo nel momento in cui è necessario cioè quando uno degli utenti collegati sta parlando. Il programma *software* per chiamate *Voip* più diffuso al mondo è *Skype*. Si precisa che si precisa che il sistema in esame, permettendo di captare anche dati criptati, consente di eseguire "intercettazioni attive": le tradizionali intercettazioni "passive" - ossia le intercettazioni del traffico dati su linea (telefonica fissa – e cellulare – definite genericamente "passive") che si basano sulla cattura del traffico duplicato dal provider di telecomunicazioni (gestore) che assicura un servizio di connettività all'indagato - non sono in grado di fornire informazioni e dati degni di interesse, in quanto la maggior parte del traffico risulta cifrato. In pratica, le intercettazioni su linea fissa (ADSL) e mobile (UMTS) permettono solo di accertare che i dispositivi in uso all'indagato sono effettivamente utilizzati, ma non consentono nella stragrande maggioranza dei casi di fornire dati rilevanti. Per tale motivo gli organismi specializzati dei servizi centrali di polizia giudiziaria, con l'ausilio di società di settore, utilizzano tecnologie in grado di intercettare le informazioni nelle fasi in cui sono in chiaro, ossia dopo la decodifica, direttamente all'interno dei dispositivi. Tali tecniche vengono generalmente denominate "intercettazioni attive", in quanto presuppongono non più soltanto un ascolto passivo del segnale, ma anche un'attività di cattura dell'informazione. Cfr. P. ANGELOSANTO, *Le intercettazioni telematiche e le criticità del* data retention *nel contrasto alla criminalità organizzata*, *Atti del convegno "Intercettazioni, tra esigenze investigative e diritto alla privacy"* – Palermo, 17-18 gennaio 2014, su *www.sicurezzaegiustizia.com.* Sul tema, esaustivamente, S. MARIOTTI-S. TACCONI, *Riflessioni sulle problematiche investigative e di sicurezza connesse alle comunciazioni* VoIP, in *Dir. interent*, 2008, p. 588 ss. Da ultimo F. CAJANI, *Le indagini informatiche per i reati di* Cyberterrorismo, in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1540 ss.; M. TORRE, *L'intercettazione di flussi telematici (art. 266-*bis *c.p.p.), ivi*, p. 1472 ss.

[50] Cass., sez. un. 13 luglio 1998, n. 21, in *Cass. pen.*, 1992, f. 2, p. 465, con nota di G. MELILLO, *L'acquisizione dei tabulati relativi al traffico telefonico fra limiti normativi ed equivoci*

Venendo alla *quaestio* relativa alla compatibilità tra le attività esperibili mediante *Trojan* impiegato in modalità di cimice informatica e le altre forme intercettive, non può sottacersi come l'attivazione del microfono sulla macchina bersaglio consenta di captare tutte le comunicazioni telefoniche che vengono effettuate tramite l'ausilio di quel dispositivo e, conseguentemente, la cimice informatica è idonea anche a captare quelle comunicazioni e conversazioni che si avvalgono della tradizionale linea telefonica nonché le comunicazioni che vengono effettuate mediante la rete internet.

Può, quindi, sostenersi che le captazioni effettuate mediante l'attivazione del microfono sul dispositivo elettronico portatile in uso all'indagato rientrano a pieno titolo nella *species* delle intercettazioni telematiche e telefoniche, tanto che la dottrina ha sostenuto che la funzione di intercettazione itinerante si confarebbe maggiormente alla disciplina di cui all'art. 266 *bis* c.p.p.[51].

Un simile approdo ermeneutico non è privo di conseguenze sul piano processuale. Infatti, poiché nel momento in cui si inocula un *Trojan* sulla macchina bersaglio non è dato sapere il tipo di comunicazione da captare, si profila il rischio, assai concreto nella prassi, che per il tramite di un'autorizzazione a procedere ad un'intercettazione ambientale mediante l'inoculazione di un *malware*, si apprenda un flusso comunicativo transitato sul dispositivo anche in via informatica.

Se è vero che le captazioni tra presenti "seguono" la disciplina di quelle telefoniche[52] e che le garanzie che presiedono tutte le *species* di intercettazione sono pressocchè identiche[53], è altrettanto incontestabile che per le operazioni di cui all'art. 266 *bis* c.p.p. cambia la tipologia di reati in presenza dei quali le stesse possono essere esperite[54].

---

giurisprudenziali; in *Guida dir*., 1998, f. 48, p. 60, con nota di R. BRICCHETTI, *Estesa la disciplina delle intercettazioni mentre la giurisprudenza si riscopre divisa*; in *Giur. it.,* 1999, f. 8, p. 1691, con nota di I. CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione ed utilizzazione delle prove cosiddette incostituzionali*. Come precisato dalla dottrina, ove è possibile l'ascolto diretto delle comunicazioni intercorrenti fra due o più interclocutori, si è in presenza di un'intercettazione disciplinata dall'art. 266 c.p.p.; quando, invece, occorra un'attività tecnica di decodificazione degli impulsi elettrici per comprendere il contenuto della comunicazione, allora la norma applicabile è quella di cui all'art. 266 *bis* c.p.p. Così L. CUOMO, *La prova digitale*, in AA. VV., *Prova scientifica e processo penale*, a cura di G. Canzio-L. Luparia, Cedam, 2017, p. 707 s. C. PARODI, VoIP, Skype *e tecnologie di intercettazione*: *quali risposte di indagine per* le *nuove frontiere delle comunicazioni*?, in *Dir. pen. proc*., 2008, f. 11, p. 1309 ss.

[51] In questo senso, S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen*. online, 2014; A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite* virus *informatico*, cit., p. 606 s.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* cit., p. 242; M. TROGU, *Le intercettazioni di comunicazioni a mezzo* Skype, in *Proc. pen. giust*., 2014, f. 3, p. 104 ss.

[52] In vista del richiamo operato dall'art. 266, comma 2 ai casi indicati dal comma 1.

[53] A meno che le captazioni ambientali non siano anche domiciliari, per cui vige una disciplina *ad hoc.* Sul punto, si rinvia a Cap. I, § ?, nt.?

[54] L'art. 266 *bis* c.p.p. ammette l'intercettazione di comunicazioni informatiche e telematiche non solo in presenza dei reati elencati dall'art. 266 c.p.p. ma anche per contrastare i reati commessi mediante l'impiego di tecnologie informatiche o telematiche. L'indicazione di questi ultimi reati ha dato luogo a dubbi interpretativi. In particolare, è stato sostenuto che essi potrebbero coincidere soltanto con i reati introdotti a seguito della l. 543/1993, ossia quelli contenuti nel Capo III, del Titolo XII, intitolato «Dei delitti contro la persona», del Libro II c.p. Si tratta degli artt. 615 *ter* («*Accesso abusivo ad un sistema informatico o telematico*»); 615 *quater* («*Detenzione e diffusione abusiva di codici di accesso a sistemi in formatici o telematici*»); 615 *quinquies* («*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*», in cui si intravede una tutela del patrimonio

Di qui, qualora l'autorità giudiziaria dovesse accogliere una richiesta di intercettazione tra presenti mediante l'attivazione di un captatore informatico su un dispositivo elettronico portatile per uno dei reati contemplati nel decalogo di cui all'art. 266, comma 1 c.p.p., risulterebbero legittimamente apprese anche le conversazioni e le comunicazioni telematiche transitanti sulla rete internet in relazione a differenti fattispecie di reato – ossia quelli commessi con l'ausilio della tecnologia informatica – che, per converso, non potrebbero consentire l'esecuzione delle intercettazioni di cui all'art. 266, comma 2 c.p.p.

A ben guardare, nessuna lesione si rinviene in ordine al disposto di cui all'art. 271, comma 1 c.p.p., che sancisce l'inutilizzabilità dei risultati delle intercettazioni disposte ed eseguite per l'investigazione di un reato non compreso negli artt. 266 e 266 *bis* c.p.p.

Come confermato dalla giurisprudenza di legittimità, ai fini dell'utilizzabilità dei risultati intercettivi nel medesimo procedimento, non rileva che all'esito delle indagini non sia stata confermata l'ipotesi di accusa per l'accertamento della quale era stato disposto il mezzo di ricerca della prova, risultando imprescindibile solo che l'attività di intercettazione sia stata autorizzata con riferimento a un delitto rientrante nella categoria dei reati per i quali il mezzo di ricerca della prova risulta consentito[55].

Dal ragionamento or ora condotto discende un corollario, a nostro avviso, difficilmente confutabile: pur non estendendo l'indagine alle altre funzioni che il captatore è in grado di svolgere una volta inoculato su un dispositivo elettronico e, dunque, limitandosi ad analizzare l'uso del *Trojan* quale cimice informatica, l'attività intercettiva scaturente dall'attivazione del microfono sulla macchina bersaglio non può trovare compiuta disciplina solo nel *dictum* di cui all'art. 266, comma 2 c.p.p., dovendo quantomeno ritenersi applicabile anche la normativa di cui all'art. 266 *bis* c.p.p.

Come già anticipato, allo stato trovano una compiuta disciplina solo le intercettazioni di comunicazioni o conversazioni tra presenti condotte mediante captatore informatico, mentre nessun cenno viene fatto alle comunicazioni informatiche o telematiche, che,

---

informatico, già protetto dall'art. 635 *bis* c.p.). In questo senso, L. UGOCCIONI, Commento all'art. 11 della l. 23/12/*93, n. 547*, in *Legislaz. pen.,* 1996, p. 57 ss.; L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 82 s. Più di recente, L. DI BITONTO, *La captazione dei flussi informatici,* in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci editore, 2018, p. 89, per cui «questa […] posizione sembra da preferire per evitare la disparità di trattamento che altrimenti si determinerebbe tra imputati dello stesso reato a seconda che esso sia stato commesso oppure no attraverso apparecchiature digitali». Tuttavia, secondo altri Autori, data la generale formulazione normativa, sembra più corretto ritenere che questa forma intercettiva possa avere ad oggetto anche i reati comuni che vengono commessi attraverso l'impiego delle tecnologie informatiche o telematiche. In questo senso, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 488 s.; A. CAMON, *Le intercettazioni nel processo penale,* cit., p. 67 s.; S.; L. LUPARIA, *Le investigazioni informatiche nell'ordinamento processuale italiano*, cit., p. 163. Più di recente, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 236.

[55] Cass., sez. IV, 28 settembre 2005, n. 47331, in *Guida dir*., 2006, f. 16, p. 100. Nello stesso senso, sez. I, 19 maggio 2010, n. 24163, in *Cass. pen*., 2011, f. 11, p. 3941, per cui «[S]sono utilizzabili i risultati delle intercettazioni disposte in riferimento ad un titolo di reato per il quale le medesime sono consentite, anche quando l'imputazione venga successivamente modificata e il giudizio di colpevolezza venga conseguentemente emesso per una fattispecie di reato per cui non sarebbe stato possibile autorizzare le operazioni di intercettazione». Sul punto, L. FILIPPI, sub *art. 266*, cit., p. 2745 s. Con precipuo riferimento alle intercettazioni mediante *Trojan*, per tutti, N. GALANTINI, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina,* in *Dir. pen. cont*., 16 marzo 2018.

dunque, non risultano essere interessate dalla riforma[56]. Il *vulnus* viene colmato dalla giurisprudenza di legittimità che ammette l'utilizzo dello strumento anche per condurre intercettazioni informatiche o telematiche[57]. Ne deriva che la collocazione delle captazioni a mezzo *virus* informatico nell'ambito delle intercettazioni di comunicazioni e conversazioni tra presenti, fornisce una copertura di facciata ad attività che, *de facto,* hanno una portata assai più ampia rispetto a quella espressamente regolamentata, con l'inevitabile conseguenza che il giudice, privo delle coordinate normative, finisce per autorizzare attività captative destinate a svolgersi in assenza del necessario bilanciamento tra gli interessi in gioco.

3. LE ALTRE FUNZIONI: ISPEZIONI, PERQUISIZIONI E SEQUESTRI INFORMATICI TRAMITE *TROJAN*

Fino a questo momento la ricerca ha avuto come oggetto solo su una delle innumerevoli funzioni che il captatore informatico è in grado di svolgere una volta inoculato sulla macchina bersaglio, ossia quella che consente l'attivazione da remoto del microfono del dispositivo infettato.

Dall'indagine condotta è emerso che l'impiego del *virus Trojan* in modalità di cimice informatica consente di condurre intercettazioni di conversazioni e comunicazioni tra presenti (art. 266, comma 2 c.p.p.), nonché intercettazioni telefoniche e telematiche "vocali" (art. 266 *bis* c.p.p.).

Arrivati a questo punto, sembra doveroso ampliare lo spettro dell'indagine, riferendosi alle altre attività, già menzionate in precedenza[58], che consistono nel «perquisire l'*hard*

---

[56] Si evidenzia, a tal proposito, la proposta dell'Avv. Stefano Aterno presentata presso la Commissione giustizia del Senato il 4 febbraio 2020, per cui sarebbe opportuna l'eliminazione della preclusione in esame in ragione delle attività – che ormai da diversi anni (Cfr. Cass., sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass*., n. 246954) – si conducono con il captatore informatico anche sui computer fissi. Cfr. S. Aterno, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, in *www.senato.it.*

[57] L'utilizzo del captatore informatico non può ritenersi escluso per le intercettazioni tra presenti che trovano luogo nei luoghi di privata dimora dove si sta svolgendo l'attività criminosa e deve ritenersi consentito per l'esecuzione di intercettazioni telematiche, *ex* art. 266 *bis* c.p.p. Così Cass., sez. V, 20 ottobre 2017, 20 ottobre 2017, n. 48370, in *Giur. it.,* 2017, n. 11, p. 2498, con nota di A. TESTAGUZZA, *Ancora in tema di captatore: le intercettazioni informatiche e telematiche. La Cassazione chiede il* bis; in *Dir. pen. proc.*, 2018, f. 8, p. 1065 ss., con nota di S. ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante* screen shot. Per un commento, v. anche C. PARODI, *Intercettazioni telematiche e captatore informatico: quali limiti?*, cit. Di qui, «sarebbe opportuno estendere la previsione normativa anche a tali tipologie di intercettazione, allo scopo di evitare inutili eccezioni sull'atipicità dello strumento in tali modalità non previste dal legislatore». Così S. ATERNO, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, cit., p. 2.

[58] Sulle in(de)finite funzioni del *virus*, si rinvia a Cap. I § 1.

disk, fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira»[59].

Andando alla "ricerca della tipicità" all'interno del codice di rito, le attività di intrusione, ricerca e acquisizione condotte attraverso il *malware* sul *device* in uso all'indagato, devono essere, *prima facie*, confrontate con le ispezioni (artt. 244 ss. c.p.p.), le perquisizioni (artt. 247 ss. c.p.p.) e il sequestro probatorio (artt. 253 ss. c.p.p)[60]. Ciò allo scopo di segnalarne affinità e differenze, giungendo alla conclusione – che qui si anticipa – che nessuno degli strumenti normati è in grado di fornire una copertura normativa alle attività investigative condotte tramite captatore informatico.

Le ispezioni (dal latino "*inspiciere*", che letteralmente significa "guardare in qualcosa") consistono nella «ricerca visiva di un possibile segno»[61], nella «osservazione della realtà di fatto quale appare all'organo che procede all'attività ispettiva»[62].

Si tratta di un'attività che si esaurisce nell'accertamento di «tracce ed effetti materiali del reato»[63] e, nel caso di dissolvimento dei segni visibili del reato, nella descrizione obiettiva dello stato dei luoghi, delle cose e delle persone.

La perquisizione (dal latino "*perquirere*", che letteralmente significa "ricercare") può essere definita come la ricerca materiale, eseguibile coattivamente su persone o luoghi

---

[59] Così Cass., sez. un., 28 aprile 2016, n. 26889, in *Arch. pen*., 2016, f. 2, p. 355.

[60] Per uno sguardo d'insieme alle sopra indicate categorie probatorie, E. APRILE, *Le indagini tecnico-scientifiche: problematiche giuridiche sulla formazione della prova*, in *Cass. pen*., 2003, f. 12, p. 4035 ss.; ID., *La prova penale*, Giuffrè, 2002; L. CARLI, *Le indagini preliminari nel sistema processuale penale*, Giuffrè, 2005, p. 319; A. FURGIUELE, *La prova per il giudizio nel processo penale*, Giappichelli, 2007; S. MAROTTA, voce *Prova (mezzi di e mezzi di ricerca della)*, in *Dig. disc. pen*., X, Utet, 1993, p. 347 ss.; M. MONTAGNA, *La ricerca della prova nelle investigazioni di polizia giudiziaria e nelle indagini Preliminari (ispezione, perquisizione e sequestro),* in AA.VV., *La prova penale*, diretto da A. Gaito, Utet, 2008, p. 96 ss.; G. TRANCHINA, *Le attività della polizia giudiziaria nel procedimento per le indagini preliminari*, in AA. VV., *Diritto processuale penale,* II, a cura di D. Siracusano-A. Galati-G. Tranchina- E. Zappalà, Giuffrè, 2011; N. TRIGGIANI, voce *Atti irripetibili*, in *Dizionario Sistematico al Codice di Procedura penale*, a cura di G. Spangher, il Sole-24 Ore, 2008, p. 651 ss.

[61] F. CORDERO, *Procedura penale*, IX ed., cit., p. 823.

[62] Così P. FELICIONI, *Le ispezioni e le perquisizioni*, Giuffrè, 2004, p. 67 s. Nello stesso senso V. GREVI, *Le prove*, in AA. VV., *Compendio di procedura penale*, a cura di Conso-Grevi, Cedam, 2014, p. 341. In generale, sulla disciplina dettata dal codice di rito vigente e per una rassegna critica dei principali orientamenti dottrinali e giurisprudenziali, C. BELLORA, voce *Ispezione giudiziale*, in *Dig. disc. pen.*, VII, Utet, 1993, p. 275 ss.; G. DEAN, voce *Ispezione giudiziale (dir. pen. proc.*), in *Enc. giur*., XX, Treccani, 1990, p. 183 ss.; S. ERCOLI, voce *Perquisizioni ed ispezioni*, in *Noviss. dig. it*., App., V, Utet, 1984, p. 860 ss.; P. FELICIONI, sub *artt. 244-246*, in *Codice di procedura penale commentato*, V ed., cit., p. 2407 ss.; ID., *Ispezioni,* in AA. VV., *La prova penale*, cit., p. 668 s.; A. MASSARI, *Ispezione giudiziale*, in *Noviss. dig. it.,* IX, Utet, 1968, p. 186 ss.; P. MOSCARINI, voce *Ispezione*, in *Enc. dir.,* Agg. II, Giuffrè, 1998, p. 464 ss.; C. PEYRON, voce *Ispezioni (dir. proc pen*), in *Enc. dir*., XII, Utet, 1972, p. 962 ss.; N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, in AA. VV., *Prove,* a cura di A. Scalfati, in *Trattato di procedura penale*, cit., p. 385 ss.

[63] Con il termine "tracce" si intendono i segni, le macchie o le impronte prodotte, direttamente o indirettamente dalla condotta delittuosa; gli "effetti materiali" sono, invece, le conseguenze o le alterazioni di natura contundente, percussiva, abrasiva, effrattiva che la stessa condotta può aver determinato su persone, cose o luoghi. In questo senso, P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 387 s.

determinati, avente la finalità di ricercare il «corpo del reato, cose pertinenti al reato»[64] ovvero la persona da arrestare[65].

Il sequestro probatorio è un mezzo di ricerca della prova che determina un «vincolo alla libera disponibilità di cose (mobili o immobili) che costituiscono corpo del reato o cose pertinenti al reato necessarie per l'accertamento dei fatti, attraverso uno spossessamento coattivo»[66].

Un'importate innovazione in tema di ispezioni, perquisizioni e sequestri è stata introdotta dall'art. 8, l. n. 48 del 2008[67], che, interpolando il contenuto di diverse norme

---

[64] Sono considerati "corpo del reato" i reperti che appartengono alla fisica del reato e pesano sull'imputato come prove a suo carico, quali l'arma del delitto, i segni contraffatti, la refurtiva, il denaro consegnato nella corruzione del pubblico ufficiale, compensi ai sicari, capitali investiti dal *racket* per riciclare il denaro di provenienza delittuosa. Sono considerate "cose pertinenti al reato" le *res* dotate di attitudine probatoria che presentano una relazione con il fatto delittuoso e sono utili o necessari alla ricostruzione dell'accaduto. Sulla nozione di corpo del reato v., per tutti, S. MONTONE, voce *Corpo del reato*, in *Dig. disc. pen*., XI, Utet, 1996, p. 155 ss.

[65] In questo senso G. BELLANTONI, sub *artt. 247-252,* in *Codice di procedura penale commentato*, V ed., cit., p. 2427 ss. Sul tema, esaustivamente, G. BELLANTONI, voce *Per*quisizioni, in *Enc. giur*., XXIII, Treccani, 1991, p. 3; P. BALDUCCI, *Perquisizioni (dir. proc. pen.),* in *Enc. dir*., XXXIII, 1983, p. 137 s.; M. BARGIS, *Perquisizione*, in *Dig. pen*. IX, Utet, 1995, P. 498 SS.; S. ERCOLI, voce *Perquisizioni ed ispezioni*, cit., p. 860 ss.; P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 70 ss.; N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 413 ss. V., in relazione al Codice del 1930, U. PIOLETTI, voce *Perquisizioni*, in *Noviss. dig. it.,* XXII, Utet, 1965, p. 1001 ss.; G. RICCIO, *Le perquisizioni nel codice di procedura penale*, Jovene, 1974; A. SCAGLIONE, *Le perquisizioni nel codice di procedura penale e nelle leggi speciali*, Cedam, 1987. Non convince, quindi, la tesi di chi ha sostenuto che le ispezioni e le perquisizioni fossero indissolubilmente legate da un «rapporto di consequenzialità». Così C. PEYRON, voce *Ispezioni (dir. proc pen),* cit., p. 965. Infatti, le ispezioni e le perquisizioni devono essere intese come attività concettualmente autonome, il cui *discrimen* è rappresentato dalla differente finalità dei due istituti: la strumentalità dell'ispezione si esaurisce nella rilevazione e descrizione di dati oggettivi, mentre la perquisizione consiste nella ricerca preordinata alla captazione. Cfr., L. CARLI, *Le indagini preliminari nel sistema processuale penale*, cit., 322. D'altra parte le due attività si differenziano anche nella prospettiva del risultato fisico delle stesse: nel caso di ispezione si tratta della scoperta di tracce od effetti materiali del reato non direttamente apprensibili ma solo documentabili; viceversa nel caso di perquisizione si tratta di una ricerca concreta di persone o cose utili per l'accertamento dei fatti. E, infatti, mentre nel primo caso l'*inspiciens* utilizza le proprie capacità sensoriali nell'esecuzione dell'attività di indagine, il perquirente si servirà delle mani al fine di impossessarsi della *res.* In questo senso L. D'AMBROSIO-P. VIGNA, *La pratica di polizia giudiziaria*, Cedam, 2003, p. 253 ss. Come anche precisato, il *perquirere* postula un «fondato motivo di occultamento del corpo del reato, di cose pertinenti al reato che giustifica l'attività di ricerca nella quale si sostanzia l'essenza stessa dell'atto»; viceversa il sequestrare presuppone la necessarietà materiale della *res* per finalità probatorie e, infatti, attraverso lo stesso si provvede ad acquisire al processo il corpo del reato o le cose ad esso pertinenti che sono palesi e «non si ritengono occultati». Così G. BELLANTONI, sub *artt. 247,* cit. p. 2429.

[66] Così N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 437. Per una panoramica dell'istituto, v. G. BELLANTONI, *Sequestro probatorio e processo penale*, La Tribuna, 2005; A. MELCHIONDA, voce *Sequestro per il procedimento penale,* in *Enc. dir.,* XLII, Giuffrè, 1990, p. 148 ss.; S. MONTONE, voce *Sequestro penale*, in *Dig. disc. pen.,* XIII, Utet, 1997, p. 253 ss.; P.P. RIVELLO, sub *artt. 253-263,* in *Codice di procedura penale commentato*, V ed., cit., p. 2453 ss.; R. SANLORENZO, sub *art. 354*, in *Commento al nuovo codice di procedura penale,* II ed., cit., p. 615 ss.; G. TRANCHINA, voce *Seque*stro, in *Enc. giur*., XXVIII, Treccani, 1992, p. 1 ss.

[67] L. 18 marzo 2008, n. 48, recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*", in *Gazz. uff*. 4 aprile 2008, n. 80. Per un quadro di insieme della l. 48 del 2008, L. CORDÍ, sub *art. 8 l. 18.3.2008, n. 43,* in *Legislaz. pen*., 2008, p. 282 ss.; R. FLOR, *Lotta alla*

del codice di rito, tenta di adeguare l'obsoleta normativa alla nuova realtà dematerializzata.

Più in particolare, con riferimento alle ispezioni, attraverso una modifica del comma 2 dell'art. 244 c.p.p., si prevede che le operazioni tecniche che l'autorità è legittimata a compiere possono avere ad oggetto anche sistemi e supporti informatici, nel qual caso è doveroso adottare «misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione»[68].

Esse consisterebbero – a differenza delle perquisizioni informatiche – in un'osservazione cui non segue l'acquisizione di dati, «essendo finalizzata esclusivamente ad accertare la presenza di dati, informazioni e programmi all'interno di un determinato supporto»[69].

---

criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet, in *Dir. pen. cont*., 20 settembre 2012; G. RESTA, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida dir*., 2008, f. 16, p. 52 ss.; ID., Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 2008, p. 2147 ss.; P. SCOGNAMIGLIO, *Criminalità informatica*. *Commento organico alla Legge 18 marzo 2008, n. 48*, Edizioni Giuridiche Simone, 2008. Sui profili processuali, S. ATERNO, *Modifiche al titolo III del libro terzo del codice di procedura penale*, in AA.VV., Cybercrime, *responsabilità degli enti, prova digitale*. *Commento alla Legge 18 marzo 2008, n. 48*, a cura di G. Corasanti-G. Corrias Lucente, Cedam, 2009, p. 193 ss.; M.L. DI BITONTO, *L'accertamento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 2008, p. 503 ss.; L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc*., 2008, f. 7, p. 717 ss.; N. VENTURA, *Ratifica della Convenzione di Budapest e iniziativa investigativa della polizia giudiziaria*, in *Giust. pen.,* 2008, f. 1, p. 225 ss.; F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.,* 2013, f. 12, p. 1259 ss. Più di recente, S. ATERNO, La convenzione di Budapest del *2001 e la L. n. 48/2008*, in AA. VV., Cybercrime. *Trattato di diritto penale*, a cura di A. Cadoppi-S. Canestrari-A. Manna-M. Papa, Utet, 2019, p. 1351 ss.; M. DANIELE, *Intercettazioni ed indagini informatiche*, in AA. VV., *Manuale di procedura penale europea*, a cura di R. E. Kostoris, 2017, p. 433 ss.

[68] Sul punto, L. CUOMO-L. GIORDANO, *Informatica e processo penale*, in *Proc. pen. giust*., 2017, f. 4, p. 716 ss.; P. FELICIONI, *Ispezioni e perquisizioni*, cit., p. 668 s.; ID., *Le ispezioni e perquisizioni di dati e sistemi,* in VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1377 ss.; N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 407 s. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 206 ss.

[69] In questo senso L. BRAGHÒ, *L'ispezione e la perquisizione di dati, informazioni e programmi informatici,* in AA.VV., *Sistema penale e criminalità informatica*, a cura di L. Luparia, Giuffrè, 2009, p. 192. Tuttavia, è stato osservato che con riferimento al digitale le caratteristiche dell'accertamento che consentono di distinguere nettamente gli istituti tradizionali della ispezione, della perquisizione e del sequestro perdono significato. Un simile rilievo critico appartiene a E. LORENZETTO, *Utilizzabilità dei dati informatici incorporati su computer in sequestro: dal contenuto al contenitore, passando per la copia,* in *Cass. pen*., 2010, f. 7, p. 1533. Infatti, osservare un *file* significa "mettere le mani" sul dispositivo di memorizzazione, quantomeno per verificarne la presenza, se non proprio per visualizzarne il contenuto, sicché in ambito informatico "osservazione e ricerca" sembrano avere il medesimo contenuto attuativo. Di qui, secondo alcuni studiosi che si sono occupati di questo fenomeno di "simbiosi" delle categorie processuali, la differenza tra ispezione e perquisizione si dovrebbe cogliere nei sistemi informatici in cui è possibile rinvenire dati coperti da credenziali di accesso e dati "liberi", cioè accessibili a qualsiasi utente abbia in uso quel determinato sistema: secondo tale opinione, rientrerebbe nell'ambito di un'attività ispettiva la visione dei *files* privi di *password*, mentre saremmo di fronte ad una perquisizione tutte le volte in cui la lettura del file richieda particolari sistemi di autenticazione. Così C. MAIOLI - E. SANGUEDOLCE, *I ''nuovi'' mezzi di ricerca della prova fra informatica forense e L. 48/2008,* in *www.altalex.com*, 30 novembre 2015. Chi non condivide tale impostazione traccia la linea di confine tra ispezione e perquisizione molto prima della lettura del file contenuto nel sistema: in una *scena criminis* informatica, l'ispezione consiste nell'osservazione del sistema informatico o telematico, nella sua descrizione, nell'elenco delle

In relazione alle perquisizioni, l'art. 8, comma 2, l. 48/2008 procede all'ampliamento delle realtà materiali su cui possono essere eseguite le attività di ricerca della prova allorquando abbia ad oggetto dati informatici[70]. In questo caso, la perquisizione si traduce nella ricerca, all'interno del dispositivo, dei *file* di interesse investigativo. La ricerca presuppone, comunque la si voglia intendere, un'intrusione all'interno del dispositivo. Ecco perché, con riferimento alla "cosa" digitale, la perquisizione deve necessariamente seguire l'apprensione (sequestro) del bene e non, viceversa, costituire attività prodromica al successivo eventuale sequestro[71].

Da ultimo, la novella interviene anche in tema di sequestro, prevedendo una peculiare disciplina allorquando l'attività di ricerca della prova inerisce a dati informatici[72].

In questo caso, i dispositivi di memorizzazione digitale delle informazioni possono rilevare sia come "corpo del reato", sia come "cose pertinenti al reato": nel primo caso, il sequestro probatorio si sostanzia nell'apprensione fisica del dispositivo *hardware*; nel secondo, invece, si traduce nella effettuazione, ove possibile, di una "copia-clone" dei dati digitali contenuti nel dispositivo, attraverso una procedura idonea ad evitare alterazioni successive, sia dell'originale che della copia[73].

---

periferiche collegate, nella specificazione di particolari sistemi *hardware* o *software* presenti, nella descrizione formale dell'eventuale sistema di connessione alla rete Internet. Propende per un simile soluzione S. ATERNO, *Modifiche al titolo III del terzo libro del codice di procedura penale*, cit., pp. 206 e ss. Per una panoramica sulle differenti ricostruzioni dottrinali in materia, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 206 ss.

[70] Ai sensi dell'art. 247, comma 1 *bis* c.p.p., «[Q]quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione». Sul tema L. CUOMO-L. GIORDANO, *Informatica e processo penale*, cit., p. 718 ss.; P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi,* in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1377 ss.; N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 430 s.; S SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 210 s.

[71] Di questa opinione, tra gli altri, L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. Legge 18 marzo 2008, n. 48. I profili processuali,* cit., p. 720, nota 19 ed E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica,* cit., p. 154.

[72] In particolare, l'art. 254 c.p.p è stato aggiornato attraverso la previsione che gli oggetti di corrispondenza possono anche essere inviati per via "telematica" e la sostituzione dei vecchi «uffici postali» con la più attuale dicitura di «coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni». Al comma 2 della medesima disposizione si specifica, inoltre, che gli ufficiali di polizia giudiziaria che procedono al sequestro non solo non possono aprire gli oggetti di corrispondenza, ma neanche alterarli. É chiaro, qui, il riferimento alla corrispondenza digitale, ontologicamente esposta, per sua natura, al rischio di contaminazione. Inoltre, è stato inserito nel codice di rito l'art. 254 *bis* c.p.p., con il quale si disciplinano le modalità del sequestro di dati informatici presso i fornitori dei servizi informatici, telematici e di telecomunicazioni. La disposizione prevede che l'autorità giudiziaria, nel disporre il sequestro dei dati, possa stabilire che l'acquisizione avvenga mediante copia su supporto informatico, «con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità». Così N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 453 s. Sul tema CUOMO-L. GIORDANO, *Informatica e processo penale*, cit., p. 719 ss.; E. NOVARIO, *Criminalità informatica e sequestro probatorio: le modifiche intorodotte dalla L. 18 marzo 2008, n. 48 al codice di procedura penale,* in *Riv. dir. proc*., 2008, f. 4, p. 1069 ss.; S. LORUSSO, *Sequestro probatorio e tutela del segreto giornalistico*, in *Giur. it.*, 2015, f. 6, p. 1504 ss. Da ultimo, A. TESTAGUZZA, *Il sequestro di dati e sistemi*, in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1437 ss.

[73] Sul tema, *amplius*, G. ZICCARDI, *Manuale breve di informatica giuridica*, Giuffrè, 2008, p. 205. Cfr.

Con il precipuo scopo di classificare le indagini svolte tramite il programma-spia, sembra opportuno distinguerne l'attività materiale dalla finalità perseguita.

Il "fine" della nuova tecnica investigativa è quello di cercare di acquisire al procedimento documenti e dati utili all'accertamento del fatto. Si converrà che si tratta del medesimo scopo che il codice di rito assegna tipicamente agli atti di ispezione, perquisizione e sequestro.

In relazione alla modalità pratiche, si osserva che il legislatore non prescrive come tecnicamente debbano essere eseguite le attività mediante *virus* informatico, lasciando ampia libertà di scelta ai soggetti del processo. Ciò vale anche nel caso in cui si tratti di ispezioni, perquisizioni e sequestri informatici, purché vengano adottate misure tecniche idonee a garantire la conservazione dei dati originali e ad impedire qualsivoglia alterazione. Di qui, sembra possibile dare esecuzione a tali istituti mediante il captatore informatico, a patto che venga assicurato il rispetto di quelle misure[74].

Prima facie, dunque, si potrebbe ritenere che le attività eseguite dal *virus* informatico presentino i caratteri propri delle ispezioni, perquisizioni e sequestri informatici, potendosi applicare anche in tali ipotesi, la disciplina relativa ai mezzi di ricerca della prova tipici.

Eppure, allorquando ci si imbatte nelle regole processuali che presidiano tali istituti, si riscontrano *impasses* non facilmente superabili. Detto in altri termini, sono le norme processuali poste a garanzia delle libertà fondamentali dei soggetti coinvolti a rappresentare un limite alla sussumibilità delle attività di intrusione, ricerca e acquisizione condotte mediante *virus Trojan* nel *genus* dei mezzi di ricerca della prova tipici[75].

Intanto, il codice prevede che l'esecuzione delle ispezioni e delle perquisizioni miri ad uno scopo ben preciso, circoscrivendo l'oggetto della "ricerca" (tracce, effetti materiali del reato). Viceversa, le attività condotte a mezzo *Trojan* prescindono dall'osservazione di tracce ed effetti materiali del reato, in quanto non sono preordinate alla ricerca del

---

anche P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi,* cit., p. 1399 ss.; A. TESTAGUZZA, *Il sequestro di dati e sistemi,* cit., p. 1449 ss. Sul tema, v. anche L. ALGERI, *Principio di proporzionalità e sequestro di sistemi informatici*, in *Dir. pen. proc*., 2020, n. 6, p. 849 s.

[74] Simili riflessioni sono svolte anche da M. TROGU, *Intrusioni segrete nel domicilio informatico*, cit., p. 576 s.

[75] In questo senso G. BONO, *Il divieto di indagini* ad explorandum *include i mezzi informatici di ricerca della prova,* in *Cass. pen*., 2013, f. 4, p. 1525 ss.; P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in. *Riv. it. sc. giur*., 2017, f. 8, p. 347 s.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* cit., p. 489 s.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, cit., p. 5 s.; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, cit., p. 349 s.; M. TROGU, *Intrusioni segrete nel domicilio informatico*, II ed., cit., p. 575 ss. *Contra* M. BONTEMPELLI, *Il captatore informatico in attesa della riforma*, cit., p. 12 s., per cui sarebbe ipotizzabile inquadrare le attività *de quibus* nella specie delle perquisizioni informatiche sulla base del rilievo per cui «l'art. 247, comma 1 *bis* c.p.p., prevedendo che la perquisizione sia disposta "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione" (analogamente dispone l'art. 244, comma 2 c.p.p., per quanto riguarda l'ispezione), demanda alla scienza e alla tecnica il compito d'individuare gli strumenti della ricerca probatoria, aprendo un varco normativo all'uso del captatore informatico concepito come apparecchiatura tecnica […]». Tuttavia, l'Autore evidenzia che «[S]si pone, però, il problema della controllabilità giudiziale dell'uso delle misure tecniche anzidette in generale, e del captatore in particolare, in funzione di garantire l'attendibilità dell'accertamento, oltre che il diritto di difesa dell'imputato».

corpo del reato o delle cose ad esso pertinenti ma dirette all'acquisizione di elementi utili a fini investigativi in un contesto spazio-temporale assai più ampio e indefinito[76].

Lo stesso discorso può farsi in relazione all'oggetto del sequestro conseguente a perquisizione: seppur la giurisprudenza in passato ha sostenuto che il provvedimento che dispone la perquisizione non debba necessariamente individuare in maniera precisa il corpo del reato o le cose ad esso pertinenti, essendo sufficiente che contenga le ragioni per cui si ha il fondato motivo di ritenere che in un determinato luogo si trovino quelle fonti di prova[77], più di recente, si è precisato che «il decreto di sequestro probatorio […] deve contenere una motivazione che, per quanto concisa, dia conto specificatamente della finalità perseguita per l'accertamento dei fatti»[78]. E comunque all'esito della perquisizione l'autorità procedente potrà legittimamente sottoporre a sequestro solo le cose utili all'accertamento del fatto e non qualsivoglia oggetto rinvenuto in loco. Insomma, «se tanto il corpo del reato che le cose pertinenti al reato possono essere sottoposti a sequestro è perché l'uno e le altre sono necessarie all'accertamento del reato»[79]. Per converso, la tecnica investigativa *de qua* prevede l'acquisizione indiscriminata di ogni documento contenuto e in futuro elaborato dal computer bersaglio, senza che vi sia la possibilità di operare una selezione tra ciò che è rilevante per le indagini e ciò che non lo è, determinando un *vulnus* al principio di proporzionalità[80].

Ma vi è di più. Una lettura costituzionalmente orientata delle norme processuali sui mezzi di ricerca della prova, che tenga conto del principio di proporzionalità nella limitazione delle libertà fondamentali, consente di individuare almeno due elementi che escludono la compatibilità delle attività con la captazione di comunicazioni e immagini a mezzo di captatore informatico.

Il primo è la temporaneità delle operazioni: l'ispezione, la perquisizione e il sequestro devono concludersi nel tempo strettamente necessario a verificare la presenza o l'assenza della fonte di prova nel luogo o sulla persona indicata nel decreto autorizzativo, ed eventualmente ad apprenderla. Di conseguenza, non può in alcun modo rientrare nel concetto di ispezione o perquisizione l'introduzione o la permanenza di un programma

---

[76] Sull'impossibilità di procedere alla perquisizione e al sequestro al di fuori dei limiti previsti dal decreto autorizzativo, Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen*., 2013, f. 4, p. 1523, cono nota di G. BONO, *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova,* cit.

[77] In questo senso Cass., sez. un., 11 febbraio 1994, n. 2, in *Giu. it*., 1994, f. 3, p. 794 ss., con nota di N. MUNCIBÍ, *Sequestro probatorio del corpo del reato e obbligo di motivazione*; in *Cass. pen*., 1994, f. 12, p. 2913, con nota di F. RIGO, *Sequestro probatorio del corpo del reato e principio della motivazione*. Nello stesso senso, sez. III, 27 settembre 2001, n. 38851, in *C.E.D. Cass*., n. 220114; sez. I, 3 ottobre 1997, n. 5545, *ivi,* n. 209889.

[78] Cass., sez. un., 19 aprile 2018, n. 36072, in *Cass. pen*., 2018, f. 12, p. 4088 ss., con nota di G. SCHENA, *Quello che le Sezioni unite non dicono a proposito di "idoneità della motivazione" nel caso di sequestro probatorio del* corpus delicti; in *Dir. pen. cont.,* 27 settembre 2018, con nota di V. GRAMUGLIA, *Le Sezioni Unite tornano sui confini dell'onere di motivazione del decreto di sequestro probatorio del* corpus delicti; in *Dir. pen. proc*., 2019, f. 2, p. 228, con nota di A. FIASCHI, *La motivazione del sequestro del corpo del reato tra vecchi dicta della Cassazione e nuova funzione nomofilattica delle Sezioni Unite*; in *Proc. pen. giust*., 2019, f. 1, p. 140, con nota di M.F. CORTESI, *Sequestro del corpo del reato e onere motivazionale: dopo un tormentato dibattito interpretativo raggiunto "forse" un punto fermo*.

[79] Così N. TRIGGIANI, *Ispezioni perquisizioni e sequestri,* cit., p. 443.

[80] Sul punto M. TROGU, *Intrusioni segrete nel domicilio informatico*, cit., II ed., p. 578 s.

spia all'interno di un computer dell'indagato, al fine di copiare e sequestrare indistintamente tutti i *file* e i dati elaborati, nonché captare le immagini e le comunicazioni realizzate attraverso l'uso dello strumento oggetto di aggressione *malware*[81].

Il secondo elemento differenziale attiene al complesso di garanzie difensive predisposto per l'esecuzione dei mezzi di ricerca della prova tipici.

In particolare, il codice garantisce il diritto di difesa prescrivendo che prima (nel caso dell'ispezione)[82], durante o dopo (nel caso di perquisizioni o sequestri)[83] il compimento dell'atto, vengano forniti avvisi alla difesa. La previsione *de qua* induce a ritenere che, per quanto le perquisizioni e i sequestri siano atti da compiere "a sorpresa"[84], la relativa disciplina rimane quella classica di "attività palese" che non può essere condotta a distanza. Il complesso di disposizioni che garantisce la posizione del destinatario della misura non può essere applicato nel caso del *Trojan*, in quanto la captazione avviene all'insaputa dell'interessato che ne resta all'oscuro per tutto il tempo della sua esecuzione.

Le differenze sostanziali che separano le attività *de quibus* rispetto ai mezzi di ricerca della prova tipici, rileva non solo nei tratti peculiari che li connotano ma anche con precipuo riferimento alla valenza probatoria del materiale probatorio raccolto. Infatti, se ispezioni, perquisizioni e sequestri sono atti irripetibili[85], la copia dei *file* memorizzati in un dispositivo informatico non richiede l'applicazione della disciplina di cui all'art. 360 c.p.p.; la Suprema Corte ha più volte escluso una simile qualificazione atteso che l'attività di riproduzione dei *files* memorizzati su un dispositivo elettronico in uso all'indagato non comporta l'alterazione, né la distruzione dell'archivio informatico che risulta consultabile ed accessibile nelle medesime condizioni, anche dopo l'intervento della polizia giudiziaria[86].

---

[81] Per approfondimenti si veda M. TROGU, *Sorveglianza e "perquisizioni"* online *su materiale informatico*, in AA. VV., *Le indagini atipiche,* a cura di A. Scalfati, Giappichelli, 2014, I ed., p. 443 ss.

[82] Ai sensi dell'art. 364 c.p.p. «[I]il pubblico ministero, se deve procedere […] a ispezione la invita a presentarsi a norma dell'articolo 375. La persona sottoposta alle indagini priva del difensore è altresì avvisata che è assistita da un difensore di ufficio, ma che può nominarne uno di fiducia. Al difensore di ufficio o a quello di fiducia in precedenza nominato è dato avviso almeno ventiquattro ore prima del compimento degli atti indicati nel comma 1 e delle ispezioni a cui non deve partecipare la persona sottoposta alle indagini. Il difensore ha in ogni caso diritto di assistere agli atti indicati nei commi 1 e 3, fermo quanto previsto dall'articolo 245 […]». Inoltre, dal momento che l'ispezione costituisce un atto al quale il difensore ha la facoltà di intervenire, sono applicabili le garanzie di cui agli artt. 366, 369 e 369 *bis* c.p.p. Pertanto, qualora l'ispezione venga disposta nel corso delle indagini preliminari, l'operazione deve essere preceduta dall'informazione di garanzia, *ex* art. 369 c.p.p. Sul tema, esaustivamente, N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 397 ss.

[83] In relazione alle perquisizioni, l'art. 250 c.p.p. stabilisce che «nell'atto di iniziare le operazioni copia del decreto di perquisizione locale è consegnata all'imputato, se presente, e a chi abbia l'attuale disponibilità del luogo, con l'avviso della facoltà di farsi rappresentare o assistere da persona di fiducia purché questa sia prontamente reperibile e idonea». In relazione al sequestro, ai sensi del comma 4 dell'art. 253 c.p.p., 4. Copia del decreto di sequestro è consegnata all'interessato, se presente. Inoltre, in base al disposto dell'art. 365 c.p.p., il destinatario della perquisizione e del sequestro viene invitato a nominare un difensore di fiducia – se ne è privo gliene viene assegnato uno d'ufficio – il quale ha diritto a partecipare al compimento dell'atto, pur senza preavviso. Cfr. N. TRIGGIANI, *Ispezioni perquisizioni e sequestri*, cit., p. 419 ss.

[84] Nel senso che il difensore non ha diritto al preavviso ma solo un diritto di assistenza.

[85] P. FELICIONI, *Le ispezioni e le perquisizioni,* cit., p. 55 ss.

[86] Così Cass., sez. V, 14 ottobre 2009, n. 16556, cit.

Dal ragionamento così condotto, consegue che l'accesso, la ricerca, la copia e l'apprensione di documenti informatici ottenuti mediante l'ausilio di un captatore informatico su di un dispositivo infettato non sia sussumibile in nessun mezzo di ricerca della prova tipizzato dal legislatore contemporaneo. Di qui, la necessità di verificare se la limitazione al diritto alla riservatezza può trovare giustificazione nel *dictum* di cui all'art. 189 c.p.p. in forza dell'atipicità delle attività investigative esperibili mediate *Trojan.*

4. L'ACQUISIZIONE DEI DATI INFORMATICI TRA SEQUESTRO DI CORRISPONDENZA E INTERCETTAZIONE TELEMATICA

Discorso a parte merita la *quaestio* relativa all'acquisizione dei dati informatici (c.d. *file*) che giacciono nella memoria o transitano su uno o più sistemi telematici allorquando il captatore informatico viene inoculato sul dispositivo oggetto di interesse.

Questo tipo di monitoraggio compiuto dal *software Trojan* può avere ad oggetto sia l'apprensione statica dei dati digitali *ivi* presenti, sia la captazione di flussi comunicativi e dati dinamici, riuscendo a intercettare conversazioni intercorrenti tra il dispositivo interessato ed altri sistemi, oppure le comunicazioni informatiche in entrata e in uscita dallo stesso.

In questo magmatico settore si profilano dubbi e perplessità circa il corretto inquadramento delle attività *de quibus*, perennemente in bilico tra differenti istituti processuali, quali le intercettazioni di flussi telematici (art. 266 *bis* c.p.p.), il sequestro di corrispondenza (art. 254 c.p.p.) e il sequestro probatorio di dati informatici (art. 253 c.p.p.).

Le maggiori difficoltà interpretative derivano dalla qualifica da attribuire ai dati informatici oggetto di acquisizione: a seconda della qualità ad essi conferita è possibile procedere alla corretta collocazione sistematica delle indagini condotte tramite *virus* informatico e, di conseguenza, verificare la legittimità dei risultati probatori ottenuti[87].

Le criticità ineriscono alla morfologia dei dati informatici di interesse investigativo (quali *e-mail*, *chat, SMS, MMS*), dal momento che molto spesso essi si presentano come documenti informatici dal contenuto comunicativo[88].

---

[87] Sul tema, diffusamente, S. ATERNO, *Acquisizione e analisi della prova informatica,* in *Dir. pen. proc.,* 2008, suppl. al f. 6, p. 62; P. TONINI, *Nuovi profili processuali del documento informatico*, in AA. VV., *Scienza e processo penale: linee guida per l'acquisizione della prova scientifica*, a cura di L. DE CATALDO NEUBURGER, Cedam, 2000, p. 436 ss. Più di recente M. TORRE, *L'intercettazione di flussi telematici (art. 266*-bis *c.p.p.),* cit., p. 1463 ss.

[88] Il documento informatico è un documento non cartaceo formato dai programmi (*software*) di un calcolatore elettronico e, contemporaneamente, alla sua formazione, registrati in un apposito spazio dal calcolatore medesimo (*hardware*) o su strumenti di supporto elettronico o digitale. Si potrebbe, dunque, definire il documento informatico come «un qualsiasi *file* avente un elemento rappresentativo espresso in un linguaggio binario». Così G. VACIAGO, *Profili processuali delle indagini informatici*, in AA. VV., *Diritto dell'internet*, a cura di G. Cassano-G. Scorza-G. Vaciago, Cedam, 2013, p. 640. Può trattarsi, quindi, di un testo, di un'immagine, di un suono, o anche di una pagina *web* o di una *e-mail*. Nello stesso senso, anche, P. CORBO, *I Documenti*, in AA. VV., *Prove,* a cura di A. Scalfati, cit., p. 317 ss.; F. RICCI, voce *Documento informatico,* in *Il diritto,* Enc. de Il Sole-24 Ore, 2007, p. 548; P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico,* in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1308 ss.; ID. *Documento informatico e giusto processo*, in *Dir. pen. proc.,* 2009, p. 401; A. VELE, *La natura delle comunicazioni contenute nella memoria del*

L'esempio tipico può essere rappresentato dalle *e-mail*, ossia «biglietti elettronici»[89] caratterizzati dalla fluidità della circolazione[90], funzionale a rinnovare gli elementi esterni delle comunicazioni e ad arricchire l'atto originariamente trasmesso senza, tuttavia, «perdere alcuna delle proprie caratteristiche»[91].

Pur essendo inquadrabili nel *genus* dei documenti informatici, si profilano evidenti difficoltà che ineriscono alla corretta individuazione degli strumenti da impiegare per prendere conoscenza del proprio contenuto[92]. Né un contributo chiarificatore arriva dalla

---

telefono cellulare nell'ambito del procedimento penale, in *Dir. inf. informatica*, 2018, f. 2, p. 285 ss. A livello di diritto interno, il legislatore, nel tentativo di definire il mezzo di prova "documento informatico", cambia impostazione diverse volte, dimostrando di non aver le idee troppo chiare sull'argomento. Nel 1993, la prima definizione di documento informatico, utile anche a fini processuali, si deve ad una esigenza tipica di diritto penale sostanziale: estendere l'incriminazione del falso documentale al dato informatico, onde evitare pericolosi vuoti di tutela. All'epoca, «[...] per documento informatico si intende[va] qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli» (cfr. art. 491 *bis* c.p., inserito dalla l. 23 dicembre 1993, n. 547). Il problema è che si è cercato di utilizzare la tradizionale definizione civilistica di documento - secondo la quale, appunto, con tale concetto si indicava un supporto -, trapiantandola senza accorgimenti nel codice penale. La conseguenza paradossale è che dal punto di vista penalistico una simile definizione di documento informatico consentiva di tutelare il solo supporto fisico e non anche il dato informatico, vero oggetto degno di tutela. «Il documento informatico contiene dati immateriali, caratterizzati dalla fragilità. Se così è, la tutela penalistica sarebbe dovuta andare oltre il supporto fisico e avrebbe dovuto proteggere il dato informatico in se stesso contro le falsificazioni». Così P. TONINI, *Documento informatico e giusto processo,* cit., p. 402. In buona sostanza, definire il documento informatico come supporto fisico significa trascurare l'elemento della rappresentazione, vero fulcro del mezzo di prova in argomento. In base a questa interpretazione, la rappresentazione di un fatto non sta nel documento, ma in colui che, leggendo il documento, formula la decisione sull'esistenza del fatto. Cfr. N. IRTI, *Sul concetto giuridico di documento*, in *Norme e fatti,* Giuffrè, 1984, p. 249). L'inidoneità di tale definizione è stata percepita dalla unanime giurisprudenza che, di fatto, l'ha ignorata completamente sino a quando è stata definitivamente abbandonata nel 2008, con la legge n. 48 del 2008. Nel frattempo, nel 2005, attraverso il Codice dell'amministrazione digitale (D. Lgs. 7 marzo 2005, n. 82), il legislatore aveva aggiornato la criticata definizione, chiarendo che per documento informatico si doveva intendere la rappresentazione informatica di un fatto giuridicamente rilevante. Il fine era buono, ma non è riuscito comunque a giustificare i mezzi: la parificazione del digitale all'analogico è avvenuta, infatti, attraverso la categoria concettuale dei "mezzi di rappresentazione". Si ritiene, invece, che l'informatica, così come la scrittura, non sono modalità rappresentative di un fatto, quanto, piuttosto, "metodi di incorporamento". Il *gap* è notevole e divide la dottrina processual penalistica. Cfr. P. TONINI, *Documento informatico e giusto processo*, cit., p. 402; G. UBERTIS, *Variazioni sul tema dei documenti*, in *Cass. pen*., 1992, f. 11, p. 2516. Di diverso avviso, P. CALAMANDREI, *La prova documentale*, Cedam, 1997, p. 10, secondo il quale «documento ai fini del processo penale deve essere considerata ogni rappresentazione, anche non intenzionale, di un contenuto probatorio incorporato, anche non durevolmente, in una base».

[89] Sono definiti così da E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, in AA. VV., *Le indagini atipiche*, cit., II ed., p. 501.

[90] Il flusso di dati codificati da elaboratori elettronici e in seguito trasmessi secondo le più evolute modalità, si trasferisce da una fonte di prova a un'altra, consentendo la fruibilità dei dati trasmessi da parte di più utenti, segnatamente il mittente, il destinatario diretto ed eventuali destinatari in copia, i quali potranno a loro volta generare un nuovo documento digitale mediante la risposta o l'inoltro di quanto ricevuto. Cfr. M. MANCUSO, *L'acquisizione di contenuti* e-mail, cit., p. 501; G. PADUA*, L'accesso alla casella* e-mail *e l'acquisizione dei contenuti: un delicato inquadramento normativo*, in *Proc. pen. giust*., 2018, f. 3, p. 590 ss.

[91] Si esprime in questo modo F. ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale*, in *Proc. pen. giust.,* 2013, f. 4, p. 106.

[92] In dottrina, P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, in AA. VV.,

giurisprudenza di legittimità che determina in modo disomogeneo la cornice giuridica alla quale ricondurre l'indagine informatica, valorizzando talvolta il ricorso al sequestro di corrispondenza (art. 254 c.p.p.)[93], talaltra, applicando la disciplina ordinaria del sequestro (art. 253 c.p.p.)[94] o, ancora, riconducendo l'acquisizione di *e-mail* già spedite o ricevute nella nozione di intercettazione di flussi telematici (art. 266 *bis* c.p.p.)[95].

Al fine di discernere la disciplina applicabile, occorre individuare correttamente "i tempi" del documento informatico, verificando se lo stesso inerisce ad una corrispondenza esaurita tra mittente e destinatario ovvero ad un flusso di comunicazioni ancora in corso: nel primo caso, si dovrà optare per l'operatività del *dictum* di cui all'art. 254 c.p.p.; nel secondo, invece, sarà applicabile la disciplina di cui all'art. 266 *bis* c.p.p.[96].

Ben più complessa appare la qualifica da attribuire ai dati informatici "statici", ossia ai messaggi di posta elettronica memorizzati in un supporto elettronico di proprietà dell'utente che giacciono nella cartella "bozze", ovvero sono inoltrati ma mai letti dal destinatario. In questi casi, potrebbe anche mancare la qualifica di "comunicazione", dal momento che il messaggio è in *stand by.*

L'intercettazione di comunicazioni, cit., p. 337 ss.; A. LOGLI, *Sequestro probatorio di un* personal computer*. Misure* ad explorandum *e tutela della corrispondenza elettronica*, in *Cass. pen*., 2008, f. 12, p. 2957 s.; E.M. MANCUSO, *L'acquisizione di contenuti* e–mail, cit., p. 505 ss.; R. ORLANDI, *Questioni attuali in tema di processo penale e informatica*, *Riv. dir. processuale*, 2009, p. 135; G. PADUA, *L'accesso alla casella* e–mail *e l'acquisizione dei contenuti: un delicato inquadramento normativo,* cit., p. 590 ss.; F. ZACCHÈ, *L'acquisizione della posta elettronica nel processo penale*, cit., p. 106 ss.

[93] Cass., sez. un. 19 aprile 2012, in *Cass. pen*., 2013, f. 7, p. 955 ss., con nota di C. RENOLDI, *Le sezioni unite sul controllo della corrispondenza di persona ristretta in istituto penitenziario.*

[94] In questo senso, Cass., sez. un., 7 settembre 2017, n. 40963, in *Dir. pen. cont*., 20 novembre 2017, con nota di G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare:* revirement *delle Sezioni Unite*; in *Cass. pen*., 2017, f. 12, p. 43, con nota di A. MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati*; in *Arch. pen*., 2018, f. 1, con nota di L. BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*; in *Cass. pen*., 2018, f. 1, p. 131 ss., con nota di P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico.* In questa pronuncia, la Corte delinea la natura del dato informatico come "cosa" sottoponibile a sequestro, a prescindere dal supporto che lo contiene.

[95] Cass., sez. III, 14 dicembre 2005, n. 12901, in *C.E.D. Cass.,* n. 231591; sez. IV, 28 giugno 2016, n. 40903, *ivi*, n. 268228. L'intercettazione del contenuto delle *e-mail* avviene tecnicamente attraverso la duplicazione dell'account oggetto di monitoraggio: si tratta di una vera e propria clonazione della cassetta di posta elettronica dell'utente con un adeguato sistema di *forwarding* presso la postazione di decodifica.

[96] Si tratta del c.d. criterio temporale, adoperato dalla dottrina per distinguere la disciplina applicabile al caso concreto, calibrato sull'attualità della comunicazione rispetto all'atto acquisitivo: l'acquisizione dinamica dei dati è inquadrata nelle intercettazioni telematiche, viceversa l'apprensione dei dati statici, una volta esaurita la funzione comunicativa, è inquadrabile nell'ambito del sequestro di corrispondenza. Cfr. E.M. MANCUSO, *L'acquisizione di contenuti* e–mail, cit., p. 505 ss.; F. ZACCHÉ, *L'acquisizione della posta elettronica nel processo penale,* cit., p. 108. Tuttavia, in considerazione della natura asincrona che può caratterizzare le comunicazioni elettroniche, la dottrina elabora anche un altro criterio, definito "funzionale" (M. PITTIRUTTI, *Profili processuali della prova informatica*, in AA. VV., *Incontri ravvicinati con la prova penale*, a cura di L. Marafioti-G. Paolozzi, Giappichelli, 2014, p. 59) o "finalistico" (P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, cit., p. 333), configurato con riguardo alle modalità occulte (intercettazione telematica) o palesi (sequestro), con cui si espleta nel caso concreto la ricerca della prova informatica.

Ferma restando la natura documentale degli stessi, negli ultimi tempi si è acuito un serrato dibattito in dottrina circa la possibilità di ricorrere alla disciplina del sequestro ovvero delle intercettazioni per acquisirne il contenuto. Sul punto, la Suprema Corte chiarisce che le *e-mail* pervenute o inviate al destinatario e archiviate nelle cartelle della posta elettronica possono essere oggetto di intercettazione, trattandosi di un flusso di dati già avvenuto ed essendo irrilevante la mancanza del presupposto della loro apprensione contestualmente alla comunicazione[97]. Esulano, invece, dal materiale intercettabile le *e-mail* "bozza", non inviate al destinatario", ma conservate nell'*account* di posta (o in apposito spazio virtuale come *Dropbox* o *Google Drive*), le quali possono comunque essere acquisite per mezzo di un sequestro di dati informatici *ex* art. 253 c.p.p., «dovendosi escludere che si tratti di corrispondenza, soggetta alla disciplina di cui all'artt. 254 c.p.p., o di dati informatici detenuti dal *provider*, sequestrabili nell'ambito della procedura prevista dall'art. 254 *bis* c.p.p.»[98].

Altrettante criticità crea l'ipotesi, tutt'altro che infrequente, dell'acquisizione dei messaggi di posta elettronica trasmessi ma temporaneamente memorizzati presso l'*Internet service provider* in attesa di essere "letti" dal destinatario.

Ebbene, la dottrina maggioritaria ritenere applicabile la disciplina di all'art. 254 *bis* c.p.p., poiché tali previsioni consentono la possibilità di sequestrare presso i fornitori di servizi telematici o di telecomunicazioni corrispondenza inoltrata per via telematica e che si deve supporre non ancora conosciuta dal destinatario[99].

---

[97] Come rileva la dottrina, l'interpretazione giurisprudenziale per cui i messaggi di posta già inviati o ricevuti dall'indagato e archiviati nelle rispettive cartelle di posta in entrata e in uscita possono essere oggetto di intercettazione a prescindere dal sistema intrusivo adottato e anche se manca la contestualità tra captazione e comunicazione, «lascia perplessi» (P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale*, cit., p. 337), dal momento che si è configurata una sorta di intercettazione che opera per il passato, nel senso che il provvedimento adottato in una certa data legittimerebbe anche le captazioni di comunicazioni avvenute in precedenza. In questo senso L. CUOMO-L. GIORDANO, *Informatica e processo penale*, cit., p. 730. D'altra parte, anche la scelta di rendere sequestrabili *ex* art. 253 c.p.p. le *e-mail* in bozza non trasmesse al destinatario è suscettibile di critiche, dal momento che «anche senza inoltro, il messaggio, il contenuto accantonato nelle bozze nasconde una vera e propria comunicazione tra gli utenti, intercettabile *ex* art. 266 *bis* c.p.p.». Così A. CAPONE, *Intercettazioni e costituzione*. *Problemi vecchi e nuovi*, in *Cass. pen*., 2017, f. 3, p. 1272 s.; M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 33. Come sostenuto, in questi casi si tratterebbe di un'intercettazione telematica *sui generis*. Infatti, pur potendo intendere il flusso comunicativo in senso ampio, i suoi confini non potrebbe essere dilatato a tal punto da ricomprendere anche i casi in cui tale flusso manchi del tutto perché la comunicazione è stata già inviata o ricevuta. Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 293.

[98] Cass., sez. IV, 28 giugno 2016, n. 40903, cit. Non solo. In quell'occasione, la Corte legittima l'uso del captatore informatico al fine di acquisire le *password* di accesso agli *account* di posta elettronica (*keylogging*), tramite cui gli inquirenti hanno preso visione sia dei messaggi che venivano via via inviati o ricevuti che di quelli salvati nella cartella "bozze". Sul punto v. *infra, § ?.*

[99] R. E. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva*, in AA.VV, *Nuove tendenze di giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* a cura di L. Ruggieri - L. Picotti, Giappichelli, 2011, p. 180. Su questo specifico aspetto, cfr. R. ORLANDI, *Questioni attuali in tema di processo ed informatica*, cit., p. 135, nonché L. LUPARIA, Computer crimes *e procedimento penale*, in AA. VV., *Modelli differenziati di accertamento,* a cura di G. Garuti, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, 2011, p. 387. *Contra* G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzie di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali,* in *Dir. inf. e informatica*, 2016, f. 1, p. 93, per cui l'acquisizione dei messaggi e-mail non ancora lette ricade nella disciplina di cui all'art.

L'approccio ermeneutico raggiunto dispiega i suoi effetti anche sull'acquisizione degli SMS (*Short messaging system*), degli MMS (*Multimedial messaging system*)[100] e dei dati trasmessi mediante "*chat*"[101]. Anche l'ipotesi di acquisizione dei dati di *chatting* oscilla tra il sequestro probatorio e l'intercettazione di comunicazioni telematiche[102].

Sul punto, si è detto che «la acquisizione di dati telematici già formati e ricevuti dal destinatario, è senz'altro maggiormente assimilabile ad una ablazione *ex* art. 254 c.p.p.»[103]; tuttavia, qualora la captazione avviene in maniera diretta, ossia «mentre il flusso scorre»[104], la stessa non può essere altro che una intercettazione di conversazioni, *ex* artt. 266 ss. c.p.p.[105].

Più di recente, la Corte chiarisce che i messaggi *WhatsApp* e gli SMS conservati nella memoria di un cellulare debbano essere considerati documenti, ai sensi dell'art. 234 c.p.p., precisando che gli stessi «non rientrano nel concetto di "corrispondenza", in quanto quest'ultima implica un'attività di spedizione in corso o comunque avviata dal mittente mediante consegna a terzi per il recapito […]» e nemmeno può ritenersi che si tratti degli esiti di un'attività di intercettazione «la quale postula, per sua natura, la captazione di un flusso di comunicazioni in corso, là invece, dove i dati presenti sulla memoria del telefono acquisiti *ex post* costituiscono mera documentazione di detti flussi»; di conseguenza l'acquisizione di tali testi non soggiace alle regole applicate per la corrispondenza e per le intercettazioni telefoniche ma alle regole di cui all'art. 253 c.p.p.[106].

---

266 *bis* c.p.p.

[100] Sul tema, *amplius*, L. FILIPPI, sub *art. 266*, cit., p. 2609; R. PANETTA, *Foto dal telefono: le misure del Garante per tutelare la riservatezza*, in *Dir. e giust*., 2003, f. 14, p. 743 ss. Da ultimo, A. TESTAGUZZA, *Il sequestro di dati e sistemi,* cit., p. 1449 ss.

[101] Si tratta, in quest'ultima ipotesi, di messaggistica istantanea (quale, ad esempio, *Messenger, Facebook, Whatsapp, Instagram, Telegram, Viber*) che viaggia in rete su canali cifrati, difficilmente penetrabili per l'indisponibilità del gestore a collaborare: di qui, l'impiego del captatore informatico rappresenta l'unica possibilità per decifrarne in tempo reale il contenuto.

[102] Sul tema, esaustivamente, A. NOCERA, *L'acquisizione delle* chat whatsapp *e* messanger: *intercettazione, perquisizione o sequestro?,* in *il penalista.it,* 12 febbraio 2018. In relazione all'acquisizione delle *chat Blackberry,* v. G. PITTELLI-F. COSTARELLA, *Ancora in tema di* chat "pin to pin" *su sistema telefonico* BlackBerry, in *Arch. pen.*, 2016, f. 1, p. 2 ss. A. TESTAGUZZA, Chat Blackberry: *si*stema "pin to pin". *Nascita di un nuovo paradiso processuale*, in *Arch. pen.,* 2016, f. 1, p. 4.; M. TROGU, *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry?, in *Proc. pen. giust*., 2016, f. 3, p. 74 ss.

[103] G. PITTELLI-F. COSTARELLA, *Ancora in tema di* chat "pin to pin" *su sistema telefonico* BlackBerry, cit., p. 3. In questo senso anche la giurisprudenza. Cfr. Cass., sez. V, 25 ottobre 2017, n. 49016, in *Proc. pen. giust*., 2018, f. 3, p. 527 ss.

[104] M. TROGU, *Come si intercettano le* chat pin to pin *tra dispositivi* Blackberry?, cit., p. 78.

[105] Cass., sez. III, 26 settembre 2019, n. 47557, in *C.E.D. Cass.*, n. 277990. Nello stesso senso sez. III, 13 maggio 2020, n. 14725, in *Proc. pen. giust.,* 13 maggio 2020.

[106] Delineano l'acquisizione delle *e-mail* quale sequestro di documenti informatici anche Cass., sez. V, 21 novembre 2017, n. 1822, in *Giur. it.,* 2018, f. 7, p. 1817 ss., con nota di M. MINAFRA, *Sul giusto metodo acquisitivo della corrispondenza informatica "statica". (Prove e messaggi telematici remoti)*, per cui «[l]i messaggi "*WhatsApp*" e gli "SMS" conservati nella memoria di un telefono cellulare sottoposto a sequestro hanno natura di documenti ai sensi dell'art. 234 c.p.p., sicchè la loro acquisizione non costituisce attività di intercettazione disciplinata dagli artt. 266 e ss. c.p.p., atteso che quest'ultima esige la captazione di un flusso di comunicazioni in atto ed è, pertanto, attività diversa dall'acquisizione "*ex post*" del dato conservato nella memoria dell'apparecchio telefonico che documenta flussi già avvenuti". Più di recente sez. III, 16 aprile 2019, n. 29426, in *C.E.D. Cass*., n. 276358; sez. VI, 28 maggio 2019, n. 28269, *ivi,* n. 276227. Ma già sez. I, 23 aprile 2014, n. 2419, *ivi,* n. 262303.

Una volta individuate le categorie probatorie che ospitano l'acquisizione dei dati informatici, il secondo passaggio logico impone di verificare la tenuta del ragionamento or ora condotto allorquando la captazione avviene mediante *virus Trojan.*

La soluzione deriva da un sillogismo quasi perfetto: se i dati informatici presentano un contenuto comunicativo "in atto", la relativa attività acquisitiva può essere inquadrata nella *species* delle intercettazioni informatiche o telematiche; di conseguenza, allorquando la captazione di tali *files* avviene mediante l'impiego dell'agente intrusore, i risultati intercettivi sono impiegabili nel procedimento penale *ex* art. 266 *bis* c.p.p., dal momento che «devono ritenersi legittime le intercettazioni informatiche o telematiche effettuate mediante l'istallazione di un captatore informatico all'interno di un computer […]»[107].

Viceversa, qualora tali dati ineriscano a documenti telematici "archiviati", la relativa attività acquisitiva configura quale sequestro di corrispondenza *ex* art. 254 c.p.p. ovvero ad un sequestro di documenti informatici, ai sensi dell'art. 253 c.p.p., qualora questi non siano mai stati spediti. Come già in precedenza chiarito[108], l'impiego del *virus Trojan* è incompatibile con l'istituto del sequestro, a fronte delle peculiarità che connotano tale mezzo di ricerca della prova. Di conseguenza, dovrebbe propendersi per l'illegittimità dei dati appresi, trattandosi di prove acquisite in violazione dei divieti stabiliti dalla legge (art. 191 c.p.p.)[109]; conclusione che può essere superata solo a patto che la nuova tecnica investigativa possa almeno ritenersi compatibile con la disciplina delle prove atipiche[110].

4.1 *SEGUE*: L'ACQUISIZIONE DEI DATI CUSTODITI NEL *CLOUD*

Nell'ambito delle investigazioni in rete, un posto di rilievo occupa la ricerca e l'acquisizione dei documenti informatici conservati nel c.d. *Cloud* (nuvola informatica).

Dal punto di vista tecnico, in prima approssimazione, può dirsi che il *Cloud* rappresenti un sistema che consente l'erogazione di servizi informatici, come l'archiviazione, l'elaborazione o la trasmissione di dati, *on demand*, attraverso la rete Internet, a partire da un insieme di risorse preesistenti e configurabili[111]. In altri termini, è il luogo (virtuale) ove possono essere allocati i dati informatici, ai quali si accede tramite dispositivi elettronici connessi alla rete o su cui si trasferiscono informazioni, foto, dati nell'ambito di un *social network*. Così, usufruendo di un simile servizio, i dati e le risorse informatiche non sono più allocate all'interno di un computer o di un dispositivo elettronico ma direttamente in rete[112].

---

[107] Cass., sez. V, 20 ottobre 2017, n. 48370, cit.

[108] Vedi *supra* §?

[109] Sul tema vedi R. DEL COCO, L'utilizzo probatorio dei *dati* Whatsapp *e* messanger *tra lacune normative* e *avanguardie giurisprudenziali*, in *Proc. pen. giust*., 2018, f. 3, p. 530 ss.

[110] Sul possibile inquadramento delle attività *de quibus* nel *genus* delle prove atipiche, v. *infra* § 5.

[111] Forniscono una simile definizione P. MELL-T. GRANCE, *The NIST Definition of Cloud Computing,* NIST*,* settembre 2011. Per i profili strettamente tecnici, si rinvia a AA. VV., *Encyclipedia of Cloud Computinh*, a cura di S. Murusegan-I. Bojanova, Jonh Wiley & Sons, 2016.

[112] Sulle caratteristiche tecniche differenziali tra informatica tradizionale e *Cloud computing*, G. GABRINI, Live Forensics *e* Cloud Computing: *due frontiere delle investigazioni digitali*, in AA. VV., IISFA Memberbook, a cura di G. Costabile-A. Attanasio, Experta, 2013, p. 147 ss.

Già dopo questa breve premessa appaiono evidenti i vantaggi connessi all'utilizzo di servizi *Cloud*: l'utente fruitore, oltre al banale utilizzo della nuvola a scopo di salvataggio remoto di dati e informazioni, può sfruttare le enormi potenzialità di *hardware* e *software* senza averne né la titolarità, né la disponibilità fisica, il tutto grazie ad una semplice connessione a banda larga.

Non si possono, tuttavia, sottovalutare le criticità derivanti dall'impiego della tecnologia: al di là delle difficoltà di ordine pratico[113], si profila il rischio, non peregrino nella prassi, della sicurezza e della riservatezza dei dati che custoditi[114], nonché questioni di competenza territoriale connesse alla mancanza di territorialità e di identificabilità tipica delle "nuvole"[115],

Dal punto di vista giuridico, in relazione alle investigazioni "tradizionali", le informazioni "esternalizzate" sono accessibili coattivamente da parte dell'autorità giudiziaria inquirente, sia tramite decreto di ispezione informatica, *ex* art. 244, comma 2 c.p.p., sia tramite decreto di perquisizione digitale, a norma dell'art. 247, comma 1 *bis* c.p.p.

Quanto all'apprensione ed al repertamento dei dati contenuti nella "nuvola", l'autorità giudiziaria può senz'altro chiedere ai gestori (fornitori di servizi informatici, telematici o di telecomunicazioni) che l'acquisizione di tali dati avvenga «mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità», così come prevede l'art. 254 *bis* c.p.p.

Nulla quaestio circa la legittimità di tali iniziative tipiche e palesi dell'autorità, a fronte delle quali peraltro il bacino di garanzie difensive è piuttosto ampio e comprende la conoscibilità dell'atto (art. 250 c.p.p.), l'assistenza del difensore (art. 365 c.p.p.) ed il deposito del verbale (art. 366 c.p.p.), con facoltà di accesso a tale atto da parte della difesa[116].

Più problematica appare, invece, l'ammissibilità di un accesso occulto alla nuvola, attraverso un *virus* di Stato.

Nei contesti di *Cloud forensics*, il captatore informatico servirebbe come strumento per perquisire non l'*hard disk* di un dispositivo elettronico ma lo stesso ambiente virtuale *Cloud*. Di qui, si potrebbe optare per la sussumibilità dell'attività *de qua* nell'ambito delle perquisizioni informatiche, la quale ricomprenderebbe anche la fase prodromica dell'accesso al servizio da parte dell'utente[117]. Tuttavia, l'incompatibilità ontologica tra le perquisizioni informatiche e le attività esplorativo-captative condotte tramite agente

---

[113] Lavorando in remoto, c'è sempre il rischio di dover subire una interruzione del servizio di *clouding*, per esempio a causa di una temporanea mancanza di linea.

[114] Cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 37.

[115] Sul tema, v. *amplius*, F. SIRACUSANO, *Prove informatiche*, in AA. VV., *Investigazioni e prove transnazionali*. *Atti del XXX Convegno nazionale dell'Associazione tra gli studiosi del processo penale*, Roma, 20 e 21 ottobre 2016, Giuffrè, 2017, p. 249 ss. Nonché S. ATERNO–M. MATTIUCCI, Cloud forensics e *nuove frontiere delle indagini informatiche nel processo penale,* in *Arch. pen*., 2013, f. 3, p. 865 ss.

[116] Sulle attività investigative tipiche condotte sul *Cloud*, v. ATERNO, Cloud forensics: *aspetti giuridici e tecnici*, in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1689 ss.; M. BONTEMPELLI, *Acquisizione dei dati custoditi nel* cloud, in AA. VV., *Le indagini atipiche*, II ed., cit., p. 589 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 35 ss.

[117] Così M. BONTEMPELLI, *Acquisizione dei dati custoditi nel* cloud, cit., p. 592

intrusore determina l'impossibilità di risolvere la *quaestio* della compatibilità tra le acquisizioni *Cloud* mediante *Trojan* e mezzi di ricerca della prova tipici nella modalità richiamata[118].

A ben guardare, la ricerca e l'acquisizione di dati informatici allocati nell'etere digitale rappresenta solo la punta dell'*iceberg* di un'attività investigativa prodromica, condotta allo scopo di recuperare furtivamente le credenziali di accesso al *Cloud*[119]. Di conseguenza, il *malware* viene impiegato per copiare tutto quanto appare sul monitor del dispositivo informatico allorquando l'utente accede ad un documento virtuale (*keylogging*)[120], in modo da venire a conoscenza delle *password* che consentiranno il successivo accesso alla nuvola informatica.

In questi termini, l'attività di ricerca e acquisizione della prova sul *Cloud* mediante ausilio del captatore informatico, lungi dal rappresentare un mezzo di ricerca della prova espressamente normato dal legislatore, deve qualificarsi quale atto atipico, salva poi la verifica della compatibilità con gli speciali criteri di ammissione *ex* art. 189 c.p.p.

5. LE ATTIVITÀ INVESTIGATIVE MEDIANTE CAPTATORE NEL *GENUS* DELLE PROVE ATIPICHE

Una volta verificata la (in)compatibilità delle indagini effettuate mediante captatore informatico rispetto alle categorie tradizionali del diritto, la ricerca prosegue tentando di rintracciare la legittimità delle investigazioni mediante captatore informatico ricorrendo alla sfumata categoria dell'atipicità. Più precisamente, è stato chiarito che, seppur potenzialmente idonee a rappresentare i medesimi risultati investigativi degli atti di indagini codificati, le attività eseguite tramite agente intrusore non esauriscono la loro portata nelle funzioni dei mezzi di ricerca della prova tipizzati, dal momento che esse o risultano ontologicamente differenti – per caratteristiche e conformazione – rispetto alle ispezioni, alle perquisizioni e ai sequestri informatici, oppure perché rappresentano strumenti di sorveglianza occulta totalizzanti per chi vi è sottoposto, differenziandosi dalle intercettazioni di comunicazioni e conversazioni tra presenti. Dunque, fallito ogni tentativo di sussunzione nelle fattispecie regolate dal legislatore, è opportuno procedere alla verifica di compatibilità con la magmatica categoria dei "mezzi di ricerca della prova atipici", in quanto nella prassi le indagini non regolate dalla legge – in specie quando si tratta di innovazioni tecnico-scientifiche – vengono legittimate ricorrendo al "parafulmine" rappresentato dall'art. 189 c.p.p.[121].

---

[118] Le ragioni che impongono di optare per una differente soluzione sono già stata esposte nel § 3, a cui si rinvia per approfondimenti.

[119] Una simile conclusione è sostenuta da E.M. MANCUSO, *La perquisizione* on line, in *Jus* online, p. 417

[120] Sulla peculiare funzione del captatore informatico, quale "specchio" riflettente le digitazioni sulla tastiera del dispositivo elettronico "infettato", si rinvia a §?.

[121] Nelle intenzioni del legislatore, la norma doveva fungere da «adattatore automatico» alle evoluzioni del tecnologico nel rispetto dei vincoli stabiliti dal diritto positivo. Così P. TONINI-C. CONTI, *Il diritto delle prove penali,* Giuffrè, II ed., 2014, p. 196. In particolare, «[L]l'art. 189 c.p.p. regola l'assunzione delle prove non previste espressamente dalla legge, così lasciando intendere che il sistema non recepisce il principio di tassatività senza peraltro ignorarne la portata garantistica. Il Progetto del 1978 aveva invece escluso l'utilizzabilità di prove atipiche od innominate nell'intento di

Tuttavia, prima di affrontare i singoli atti investigativi che possono rappresentare "modelli" atipici già sperimentati dal sistema giuridico, occorre soffermarsi sulla configurabilità di questa anomala categoria probatoria di completa elaborazione giurisprudenziale[122].

Sulla prospettabilità dei mezzi di ricerca atipici della prova, la dottrina avanza delle perplessità[123].

Intanto, ci si chiede se gli organi inquirenti siano vincolati al compimento di atti di indagine espressamente disciplinati dalla legge oppure possano compierne di altri. Le disposizioni codicistiche che regolano l'attività del p.m. e della p.g. fanno propendere per la seconda soluzione[124]. Infatti, l'art. 55 c.p.p. assegna alla p.g. il potere-dovere di svolgere, di propria iniziativa o su delega del p.m., ogni attività finalisticamente orientata ad assicurare le fonti di prova e a raccogliere quant'altro possa servire per l'applicazione della legge penale[125]; di conseguenza, possono essere compiuti sia atti tipici (artt. 349-

---

rafforzare le garanzie difensive dell'imputato in relazione a mezzi di accertamento dei fatti di reato la cui acquisizione potrebbe condurre ad errori o abusi (ad es. tavole d'ascolto idonee ad intercettare conversazioni tra presenti). Riesaminatosi il problema in tutti i suoi profili di politica e tecnica processuale, si è scelta una strada intermedia che consente al giudice di assumere prove non disciplinate dalla legge ma lo obbliga a vagliare, a priori, che queste siano, al tempo stesso, affidabili sul piano della genuinità dell'accertamento e non lesive della libertà morale della persona. Verificata l'ammissibilità del mezzo di prova atipico, il giudice dovrà poi regolarne in concreto le modalità di assunzione così da rendere conoscibile in anticipo alle parti l'iter probatorio». Cfr. *Relazione al progetto preliminare del codice di procedura penale del 1988*, in *Gazz. uff*., 24 ottobre 1988 n. 250, suppl. ord. n. 2, p. 60. In tema v. anche V. GREVI-G.P. NEPPI MODONA, Introduzione al progetto preliminare del 1988, in *Il nuovo codice di procedura penale dalle leggi delega ai decreti delegati*, vol. IV, Cedam, 1990, p. 553; M. NOBILI, *La nuova procedura penale. Lezione agli studenti,* Il Mulino, 1989, p. 100. Sul tema della prova atipica, la dottrina è assai vasta. Solo a titolo esemplificativo, E. AMODIO, *Libero convincimento e tassatività dei mezzi di prova: un approccio comparativo*, in *Riv. it. dir. proc. pen.,* 1999, f. 1, p. 3; V. BOZIO, *La prova atipica*, in AA. VV., *La prova penale*, cit., p. 57 ss.; M. CONTE-M. GEMELLI-F. LICATA, *Le prove penali*, Giuffrè, 2011, p. 35 ss.; C. CONTI, sub *art. 189*, in *Codice di procedura penale commentato,* cit., p. 1880 ss.*;* ID., voce Prova atipica, in Procedura penale. Dizionari sistematici, a cura di G. Spangher, Il Sole 24 Ore, 2008, p. 360 ss.; A. LARONGA, *Le prove atipiche nel processo penale*, Cedam, 2002, p. 6 e ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p.108 ss.; M. NOBILI, sub *art. 189 c.p.p.,* in *Commento al nuovo codice di procedura penale*, cit., p. 398; C. PANSINI, *É valida la prova atipica senza la preventiva audizione delle parti?,* in *Dir. pen. proc.,* 1997, f. 11, p. 1257; G.F. RICCI, *Le prove atipiche*, Giuffrè, 1999, p. 46 ss.; G. TABASCO, *Prove non disciplinate dalla legge nel processo penale. Le "prove atipiche" tra teoria e prassi*, Edizioni Scientifiche italiana, 2011, p. 13 ss.; P. TONINI-C. CONTI, *Il diritto delle prove penali*, cit., p. 185 e ss.; ZACCHÈ, *La prova atipica*, in *Dig. proc. pen.* online, diretto da Scalfati, Giappichelli, 2012.

[122] Cass., sez. un., 28 luglio 2006, n. 26795, in *Arch. nuova proc. pen*., 2006, f. 6, p. 621 ss. Per una disamina delle videoriprese investigative quale mezzo di ricerca della prova atipico, si rinvia a § ?. Nello stesso senso, in relazione alla localizzazione da remoto a mezzo di sistema di rilevamento GPS, da ultimo, Cass., sez. II, 4 aprile 2019, n. 23172, in *C.E.D. Cass*., n. 262966.

[123] Per una ricostruzione dettagliata degli orientamenti dottrinali sul punto, V. BOZIO, *La prova atipica*, cit., p. 57; C. CONTI, sub *art. 189*, cit., p. 1880 ss.; ID., voce *Prova atipica*, cit., p. 360 ss.; A. LARONGA, *Le prove atipiche nel processo penale*, cit., p. 55 ss.

[124] In questo senso A. SCALFATI-D. SERVI, *Premesse sulla prova penale*, in AA. VV., *Prove,* cit., p. 32

[125] Sul punto, G. AMATO–M. D'ANDRIA, *Organizzazione e funzioni della polizia giudiziaria nel nuovo codice di procedura penale*, Giuffrè, 1990, p. 23 ss.; G. BRUNO, voce *Polizia giudiziaria*, in *Enc. dir*., XXXIV, Giuffrè, 1985, p. 159 ss.; G. CASACCIA, sub *art. 55*, in *Codice di procedura penale commentato*, V ed., cit., p. 747 ss.; E. CESQUI, sub *art. 55,* in *Commento al nuovo codice di procedura penale*, II ed., cit., p. 729 ss.; L. D'AMBROSIO–P.L. VIGNA, *La pratica di polizia giudiziaria*, Cedam, 2007, p. 418 ss.;

352 e 354 c.p.p.), sia atti atipici non disciplinati nel loro contenuto. D'altra parte, l'art. 348 c.p.p. prevede che il p.m. sia legittimato a svolgere ogni attività necessaria – anche atipica – al fine di assumere le determinazioni inerenti all'esercizio dell'azione penale[126].

Chiarito l'aspetto dell'apertura codicistica al mondo dell'inedito, la seconda perplessità deriva dall'interpretazione dell'art. 189 c.p.p. che provvede a regolare solo le "prove" atipiche, mentre nessun richiamo espresso è manifestato in ordine ai mezzi di ricerca della prova[127]. Di qui, la dottrina pone delle riserve circa l'applicabilità della norma "in bianco" anche a tali categorie probatorie, a fronte dell'impossibilità ontologica di garantire il rispetto dei requisiti *ivi* indicati[128]. In particolare, l'orientamento minoritario – che nega tale categoria – rileva l'impossibilità di estendere la portata dell'art. 189 c.p.p. anche ai mezzi di ricerca della prova esperiti nel corso delle indagini, in quanto si tratta di prove precostituite rispetto all'istruzione dibattimentale che, di norma, vengono acquisite a sorpresa. Non sarebbe, quindi, possibile dare completa attuazione all'art. 189 c.p.p., nella parte in cui impone al giudice di sentire le parti sulle modalità di assunzione della prova, prima di decidere con ordinanza sulla richiesta di

---

P. DORIGO, voce *Polizia giudiziaria*, in *Noviss. dig. it.,* Utet, 1984, p. 1034 ss.; S. GIAMBRUNO, voce *Polizia giudiziaria*, in *Dig. disc. pen*., IX, Utet, 1995, p. 597 ss.; P. GROSSO, voce *Polizia giudiziaria*, in *Enc. giur.,* XXIII, Treccani, 1990, p. 27 ss.; A. MORGIGNI, *L'attività della polizia giudiziaria*, Giuffrè, 2002; P. TONINI, *Polizia giudiziaria e magistratura, profili storici e sistematici*, Giuffrè, 1979.

[126] Sul tema G. AMATO–M. D'ANDRIA, *Organizzazione e funzioni della polizia giudiziaria nel nuovo codice di procedura penale*, cit., p. 89 ss.; L. BRESCIANI, sub *art. 348*, in *Commento al nuovo codice di procedura penale*, II ed., cit., p. 136 ss.; F. CASSIBBA, voce Investigazioni e indagini preliminari, in *Dig. disc. pen*., Agg., Utet, 2004, p. 509 ss.; A. CHELO, Le prime indagini preliminari sulla scena del crimine, Cedam, 2013; D. CURTOTTI–L. SARAVO, *Il volo di Icaro delle investigazioni sulla scena del crimine: il ruolo della polizia giudiziaria,* in AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi*, a cura di C. Conti, Giuffrè, 2011; P.P. PAULESU, sub art. 348, in *Codice di procedura penale commentato*, V ed., cit., p. 393 ss.; P. VOENA, voce *Investigazioni ed indagini preliminari,* in *Dig. disc. pen*., VII, Utet, 1993, p. 264 ss.

[127] La distinzione tra mezzi di prova e mezzi di ricerca della prova è motivata nella Relazione al progetto preliminare del codice di procedura penale sulla base di un duplice profilo: da un punto di vista logico, i primi si caratterizzano «per l'attitudine ad offrire al giudice risultanze probatorie direttamente utilizzabili in sede di decisione», i secondi, invece, «rendono possibile acquisire cose materiale, tracce o dichiarazioni dotate di attitudine probatoria»; sotto il profilo tecnico–operativo, mentre i mezzi di prova sono assunti con la piena attuazione del contraddittorio, in dibattimento o nell'incidente probatorio, i mezzi di ricerca della prova si caratterizzano come attività basate sull'effetto "sorpresa", trattandosi di casi in cui la prova è precostituita e non deve, perciò, essere formata durante il processo. Cfr. *Relazione al progetto preliminare del codice di procedura penale*, cit., p. 70 ss. In dottrina, *ex plurimis*, AA. VV., *Giurisprudenza sistematica di diritto processuale* penale, diretta da E. MARZADURI–M. CHIAVARIO, vol. III, *Le prove*, t. II, *I singoli mezzi di ricerca della prova*, coordinato da E. MARZADURI, Utet, 1999; A. BARGI–S. FURFARO, *Le intercettazioni di conversazioni e di comunicazioni*, cit., p. 109 ss.; P. FERRUA, La prova nel processo penale, Giappichelli, 2017, p. 132 ss.; A. FURGIUELE, *La prova nel processo penale: formazione, valutazione e mezzi di ricerca della prova*, Giappichelli, 2007, p. 150 ss.; S. MAROTTA, *voce (mezzi di e mezzi di ricerca della),* in *Dig. disc. pen*., X, Utet, p. 347 ss.; M. RUOTOLO, *Regolazione dei mezzi di ricerca della prova e sindacato della Corte costituzionale,* in *Quad. cost*., 2017, f. 2, p. 367 ss.; P. TONINI–C. CONTI, *Il diritto delle prove penali*, II ed., cit., p. 413 ss. Ne fa una distinzione di natura ideologica. F. CORDERO, *Tre studi sulle prove penali*, cit., p. 67 s.

[128] L'art. 189 c.p.p. consente l'ingresso nel processo di prove atipiche, purchè ciò avvenga nel rispetto di precise condizioni: idoneità ad assicurare l'accertamento dei fatti; rispetto della libertà morale dell'individuo; tutela del contraddittorio. Sul punto C. CONTI, sub *art. 189*, cit., p. 1885 ss.

ammissione[129]. La dottrina maggioritaria propende, tuttavia, per un'interpretazione "elastica" della norma: qualora si tratti di mezzi di ricerca della prova atipici, anziché configurare un contraddittorio anticipato sull'ammissione in corso, si dovrà svolgere un contraddittorio successivo sulla utilizzabilità degli elementi acquisiti[130]. Dunque, pur ammettendo l'estensione della "valvola di sicurezza" della prova atipica ai mezzi di ricerca della prova, anche per l'acquisizione di questi ultimi devono essere rispettati i precisi parametri stabiliti dall'art. 189 c.p.p.

Nel caso dei *Trojan*, è fuori discussione che si tratti di prove idonee ad assicurare l'accertamento dei fatti. Inoltre, l'utilizzo del *virus* informatico non sembra in grado di "pregiudicare la libertà morale" (*id est*, di condizionare i comportamenti) delle persone coinvolte nell'indagine. Quanto alla necessità di «sentire le parti sulle modalità di assunzione della prova», è pur vero che un interpello preventivo dell'indagato non è in questo caso ipotizzabile, trattandosi di attività investigative occulte, ma, come anticipato, l'art. 189 c.p.p. può dirsi rispettato anche se il contraddittorio sulle modalità acquisitive della prova avviene *a posteriori*, al momento dell'utilizzo dibattimentale dei materiali probatori ottenuti per mezzo dello strumento atipico di ricerca della prova.

In linea di principio, dunque, le indagini svolte per mezzo dei captatori informatici possono ritenersi in linea di principio qualificabili quali atti di indagini atipici e, di conseguenza, ammissibili anche se non regolati espressamente dalla legge[131].

6. LE PERQUISIZIONI *ONLINE*

Rispetto alle funzioni del captatore informatico, la vera criticità risiede in quelle attività di ricerca che, servendosi delle moderne tecnologie di rete, possono svolgersi da

---

[129] Così N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992, p. 213. Ulteriori perplessità sul tema sono rilevate da G. LEONE, *Trattato di diritto processuale penale*, Jovene, 1961, p. 178, secondo cui «[Q]quando il codice nella sua ben architettata struttura prevede un quadro di mezzi di prova, è intorno ad esso che deve roteare la vicenda giudiziaria; essendo evidente, tra l'altro, che la mancata previsione di un mezzo di prova sta a significare che le prospettive di politica criminale che hanno presieduto alla formazione della legge lo hanno escluso; e che anche in caso di sopravvenuto delinearsi di un nuovo strumento di acquisizione della prova non è l'interprete, bensì il legislatore a dover aggiornare il sistema». La preoccupazione nell'ammettere prove *extra* catalogo legale era di veder compromessi in tal modo i diritti dell'imputato. Cfr. G. CONSO, *La natura giuridica delle norme sulla prova ne processo penale,* in *Riv. dir. proc*., 1970, f. 1, p. 20; E. ZAPPALÁ, *Il principio di tassatività dei mezzi di prova nel processo penale*, Giuffrè, 1982. p. 99 ss.

[130] In dottrina, A. CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionale*, in *Cass. pen.,* 1999, f. 10, p. 1195 s.; L. FILIPPI, L'home watching*: documento, prova atipica o prova incostituzionale?,* in *Dir. pen. proc*., 2001, f. 1, p. 92; G.F. RICCI, *Le prove atipiche*, cit., p. 538 ss.; A. SCALFATI-D. SERVI, *Premesse sulla prova penale*, cit., p. 32 ss. Sembrano orientarsi in questo senso le sezioni Unite della Cassazione. Cfr. Sez. un., 28 luglio 2006, n. 26795, cit., in cui la Corte Suprema ha provveduto a distinguere tra mezzo di ricerca, elemento e mezzo di prova: «[..]il contraddittorio previsto dall'art. 189 c.p.p. non riguarda la ricerca della prova, ma la sua assunzione e interviene, dunque, come risulta chiaramente dalla disposizione, quando il giudice è chiamato a decidere sull'ammissione della prova».

[131] Optano per una simile scelta, A. CAMON, *Cavalli di Troia in Cassazione,* cit., p. 91; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* cit., p. 485 ss.; E.M. MANCUSO, *L'acquisizione di contenuti* e-mail, cit., p. 501; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 309.

remoto per carpire le più svariate informazioni transitanti o giacenti nel dispositivo infettato.

Il riferimento va a tutte quelle tecniche di occulta intrusione nei sistemi informatici che consentono di captare dati statici memorizzati dall'utente e monitorare il dispositivo infetto al pari del *controller* e che rientrano – secondo la dottrina maggioritaria[132] – nella magmatica categoria delle c.d. perquisizioni *online*[133].

Si tratta di «un mezzo di indagine che consente di effettuare un insieme di operazioni all'insaputa dell'interessato, volte sia a esplorare un sistema informatico per trarne utili elementi probatori, sia a monitorarlo con costanza»[134] e, più precisamente, di «un'attività investigativa che assomma le caratteristiche e le funzioni di diversi mezzi di ricerca della prova tipici, pur non essendo riconducibile ad alcuno di essi, e che presenta altresì caratteri di originalità»[135].

Non deve trarre in inganno l'uso della parola "perquisizioni" nella denominazione, poiché rispetto al già noto istituto, questo «è di gran lunga più "aggressivo"»[136], caratterizzandosi per il suo carattere occulto, perdurante nel tempo e per la circostanza che consente di lucrare una massa di risultanze assai più cospicua rispetto a quella ottenibile mediante l'esperimento del tradizionale mezzo di ricerca della prova.

È attorno a un doppio nucleo di attività, ricognitive e "*live*", che gravitano le diverse situazioni prospettabili, basate, da una parte, sulla raccolta dei dati immagazzinati nel *device*, dall'altra, sull'operato di una "spia" onnipresente, celata nel cellulare sempre al seguito dell'utente.

---

[132] In questo senso P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 347 ss.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia,* cit., p. 485 ss.; P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale,* in AA. VV., *L'intercettazione di comunicazioni*, cit., p. 303 ss.; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 309 ss.; M. TORRE, *Le intercettazioni a mezzo del c.d. captatore informatico o "*trojan *di Stato*", in AA. VV., Cybercrime. *Trattato di diritto penale*, cit., p. 1660 ss. Contraria a tale impostazione S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 291, per cui «si tratta di una denominazione che coglie al più una delle possibili sfaccettature dell'utilizzo del *Trojan* che si presta ad una molteplicità di impieghi».

[133] Sull'istituto delle perquisizioni *online*, esaustivamente, E.M. MANCUSO, *La perquisizione* on line, cit., p. 412 ss.; L. PARLATO, voce *Perquisizioni* on line, in *Enc. dir*., Annali, X, Giuffrè, 2017, p. 601 ss.; EAD., *Problemi insoluti: le perquisizioni* on-line, cit., p. 308 ss.

[134] Così L. PARLATO, voce *Perquisizioni* on line, cit., p. 601.

[135] L'espressione appartiene a P. FELICIONI*, Le perquisizioni*, in AA. VV., *La prova penale*, cit., p. 697. Nello stesso senso F. IOVENE, *Le c.d.* perquisizioni online, in *Dir. pen. cont*., 2014, f. 3-4, p. 16. Il fatto che le perquisizioni *online* non siano riconducibili ad alcuno dei mezzi di ricerca della prova specificamente disciplinati dal codice di rito non significa che si possa automaticamente concludere nel senso della loro ammissibilità alle condizioni stabilite dall'art. 189 c.p.p. quale prova atipica. Infatti, il primo presupposto di validità di una prova atipica è la sua legittimità costituzionale. Violando gli artt. 14 e 15 Cost., nell'assenza di una specifica disciplina legislativa, le c.d. perquisizioni *online* darebbero vita ad una prova inutilizzabile in quanto incostituzionale. Cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 557 ss. Si potrebbe propendere per l'inammissibilità, se si accoglie l'idea, di marca giurisprudenziale, che l'art. 189 c.p.p. presuppone la formazione lecita della prova e che quindi nel caso delle attività atipiche il vaglio di ammissibilità è attività preliminare e precede quello di inutilizzabilità. S. MARCOLINI, *Le cosiddette perquisizioni* online, in *Cass. pen.,* 2010, f. 12, p. 2855 ss.

[136] L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 295.

In quest'ottica, si tende a differenziare due tipologie di manovre investigative, costituite rispettivamente da *online search* (copiatura) e *online surveillance* (appostamento e monitoraggio)[137].

Nella prima categoria vengono incluse le indagini dirette a frugare a distanza e occultamente all'interno della memoria di massa del dispositivo infettato, permettendo all'investigatore di far copia, totale o parziale, dei dati memorizzati dall'utente.

Attraverso un'attività investigativa di questo tipo, gli inquirenti sono in grado di effettuare non solo ricerche "mirate", funzionali all'acquisizione di elementi di prova utili alle indagini, ma anche "massive", al fine di venire a conoscenza di tutte le informazioni digitali archiviate nel sistema[138].

Nonostante le resistenze della dottrina dominante[139] – che contesta la legittimità costituzionale di tali attività investigative –, la giurisprudenza tende ad inquadrare la nuova tecnica di indagine nel *genus* della prova atipica[140].

---

[137] In questo senso M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 12 s.; R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, cit., p. 222. Secondo G. ZICCARDI, *Parlamento Europeo, captatore informatico e attività di* hacking *delle Forze dell'Ordine: alcune riflessioni informatico-giuridiche,* in *Arch. pen.,* 2017, f. 1, p. 1, le operazioni tecniche effettuabili per mezzo dell'agente intrusore potrebbero suddividersi in tre macro-aree, riconducibili: 1) al controllo dell'*hardware* del dispositivo; 2) al controllo dei contenuti del dispositivo; 3) all'acquisizioni di informazioni scambiate sul dispositivo. Secondo L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 308 ss., esistono diversi gradi dell'atipicità - rappresentati da una sorta di centri concentrici più o meno distanti dal nucleo centrale delle attività più prossime alle intercettazioni di comunicazioni. La stessa individua un tasso di atipicità crescente nelle seguenti categorie: intercettazioni *sui generis*, ossia quelle ambientali con captatore informatico disciplinate nel 2017; zona grigia che raccoglie ipotesi di investigazioni con *virus Trojan* spesso riconducibili a fattispecie investigative tipiche; attività di perquisizioni *on line* più periferiche rispetto alle intercettazioni; altre attività atipiche costituenti espressione sia di *on line search* sia di *on line surveillance*. Secondo l'Autrice, il *discrimen* da effettuare è solo legato al binomio intercettazioni-perquisizioni online, per cui «è in esito ad una sorta di sottrazione che può parlarsi di perquisizioni *on line*, dovendosi indicare con questa espressione tutto ciò che è accessibile attraverso lo strumento del *Trojan* al netto delle intercettazioni». Sul punto, v. anche Cap. I, § 1.

[138] Sul tema, cfr. M. TORRE, *Il captatore informatico tra riforma Orlando e sistema processuale*, in *Giur. it*., 2018, f. 7, p. 57 ss.

[139] In questo senso P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale,* cit., p. 303 ss.; E.M. MANCUSO, *La perquisizione* on line, cit., p. 412; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, cit., p. 308 ss., M. TROGU, *Intrusioni segrete nel domicilio informatico*, II ed., cit., p. 579 ss. *Contra* R.O. VALLI, *La perquisizione informatica e la perquisizione da remoto*, in *Il Penalista*, 18 ottobre 2017, per cui tali attività rientrano nella sfera di copertura dell'art. 189 c.p.p.

[140] Cass., sez. V, 14 ottobre 2009, n. 16556, cit. Per commenti, M.T. ABBAGNALE, *In tema di captatore informatico*, cit., p. 2 s.; S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ss.; ID., *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del* cloud criminal, cit., p. 7.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, cit., p. 8; P. FELICIONI, *L'acquisizione da remoto dei dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, cit., p. 128; L. GIORDANO, *La disciplina del "captatore informatico"*, in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci, 2018, p. 250; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 314 s.; A. TESTAGUZZA, voce Virus *informatico,* cit., p. 932 s.; ID., *Exitus acta probat "Trojan" di Stato: la composizione di un conflitto,* in *Arch. pen.,* 2016, f. 2, p. 9 ss. Sul punto, v. Cap. I, § 2. In una isolata pronuncia, la Corte propende per l'inutilizzabilità del materiale acquisito tramite la tecnica investigativa esplorativa. Cfr. Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen.*, 2013, f. 12, p. 1523

Considerazioni non dissimili valgono per la seconda *species* di attività afferente al *genus* delle perquisizioni *online*: tramite i programmi spia che realizzano la c.d. *online surveillance*, è possibile monitorare il flusso di dati che intercorrano tra periferiche (come video, tastiera, microfono e *webcam*) e microprocessore del dispositivo sorvegliato, con un controllo immediato e continuativo[141]. Si pensi, solo a titolo esemplificativo, alla possibilità di captare tutto il traffico in arrivo o in partenza dal dispositivo infettato (navigazione e posta elettronica sia *web mail*, sia *out l*ook) (intercettazione telematica); attivare il microfono del dispositivo infetto e così apprendere i colloqui che si svolgono nello spazio circostante il soggetto che ha in uso il dispositivo, ovunque si trovi (intercettazione ambientale); mettere in funzione la web camera, consentendo di captare le immagini (videoriprese); decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e tutto ciò che compare sullo schermo (*screenshot*).

Ogni singola attività può costituire sia un'attività investigativa atipica autonoma oppure rappresentare il frutto di un'indagine assai più complessa, ossia un segmento in cui si scompone la perquisizione on line, allorquando il *Trojan* funge da *panopticon*[142].

Anche in questi casi, nonostante la maggiore incisività delle attività in esame risetto alle prerogative individuali inviolabili, la giurisprudenza propende per la legittimità dei risultati investigativi appresi, ricorrendo talvolta alla atipicità della prova[143], talaltra alla categoria tipica delle intercettazioni telematica[144], altre volte ancora servendosi di entrambi gli istituti giuridici a seconda dell'oggetto dell'acquisizione[145].

---

ss. In quell'occasione, la Suprema Corte ha confermato l'annullamento da parte del Tribunale del riesame del decreto di perquisizione e sequestro. Infatti, la Suprema Corte ravvisa in simile provvedimento un inammissibile strumento a carattere esplorativo, «che mirava non tanto ad acquisire elementi di conoscenza in ordine ad una o più *notitiae criminis* determinate, quanto a monitorare in modo illimitato, preventivo e permanente il contenuto di un sistema informatico onde pervenire per suo tramite all'accertamento di reati non ancora commessi, ma dei quali si ipotizzava la futura commissione da parte di soggetti ancora da individuarsi». Pertanto, conclude la Corte, «è da escludere un preventivo ed indefinito monitoraggio del sistema predetto in attesa dell'eventuale e futura comparsa del dato da acquisire a base delle indagini: si verrebbe altrimenti ad integrare un nuovo ed anomalo strumento di ricerca della prova, con finalità nettamente esplorative, di mera investigazione (paragonabile alle intercettazioni), che nulla ha a che fare con la perquisizione». Per commenti, G. BONO, *Il divieto di indagini* ad explorandum *include i mezzi informatici di ricerca della prova*, in *Cass. pen.,* 2013, f. 4, p. 1523 ss.; G. CORRIAS, *Perquisizione e sequestro informatici: divieto di* inquisitio generalis, in *Dir. inf. e inf.*, 2012, f. 6, p. 1146 ss.

[141] Sul punto S. MARCOLINI, *Le cosiddette perquisizioni* online, cit., p. 2859.

[142] Cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 294.

[143] Come nel caso dell'attivazione del GPS satellitare. Solo per citare alcuni esempi, Cass., sez. V, 10 marzo 2010, n. 9667, in *Dir. pen. proc.*, 2010, p. 1464 ss.; sez. II, 13 febbraio 2013, n. 21644, in *CED Cass.*, n. 255542; sez. II, 4 aprile 2019, n. 23172, cit. Sul punto e per una panoramica delle differenti posizioni giurisprudenziali, si rinvia a nt. 157.

[144] Così la Corte configura l'attività di investigazione conseguente al *keylogging* o agli *screenshots*. Cfr. Cass., sez. IV, 28 giugno 2016, n. 40903, cit.; sez. V, 21 novembre 2017, n. 1822, cit.

[145] Come è accaduto nel caso delle videoriprese investigative. Cfr. Cass., sez. un., 28 luglio 2006, n. 26795, cit.

6.1. *SEGUE*: IL PEDINAMENTO "INFORMATICO" TRAMITE *TROJAN*

Il pedinamento elettronico rappresenta «un'attività di monitoraggio tecnologicamente avanzata che, con meccanismi di localizzazione satellitare, consente di tracciare gli spostamenti di un veicolo o di una persona "a distanza"»[146], sfruttando il sistema di posizionamento geografico GPS (*Global Positioning System*) in grado di rilevare, in tempo reale, le coordinate spazio–temporali in qualsiasi punto esso si trovi.

La peculiarità di questa *species* di geolocalizzazione è l'osservazione in tempo reale del movimento del soggetto "sul" quale è stato installato in maniera occulta l'apparecchio che rileva le posizioni e le coordinate spazio-temporali relative agli spostamenti[147]. L'utilizzo investigativo di questo tipo di monitoraggio non necessita di supporti "esterni": è sufficiente che la persona da monitorare porti con sé, nei suoi spostamenti, lo *smarthphone* o il *tablet* dotato di connessione mobile affinchè gli investigatori possano conoscere i movimenti del soggetto senza limiti spazio-temporali.

Negli ultimi tempi, gli inquirenti si avvalgono dei sistemi di geolocalizzazione degli apparati mobili cellulari e degli *smarphon*, sfruttando le potenzialità ontologiche del captatore informatico per introdursi nel dispositivo ed attivare il GPS satellitare dello stesso ai fini di monitoraggio.

A ben guardare, la tecnica investigativa in esame può essere ricompresa nell'ambito della *on line surveillance*, con la caratteristica che in tal caso è (anche) il soggetto "persona-fisica" ad essere oggetto di monitoraggio e non (solo) il dispositivo infetto. Ebbene, se dal punto di vista tecnico-operativo gli strumenti di sorveglianza ad alto contenuto tecnologico risultano assai utili nell'accertamento del fatto di reato,

---

[146] Così M. STRAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prospettiva atipica*, in *Dir. pen. proc*., 2011, f. 12, p. 2013. Nello stesso senso T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* in AA. VV., *Le indagini atipiche*, II ed., cit., p. 443.

[147] Da questa ipotesi deve distinguersi il caso in cui sugli apparati si prelevano i dati in un momento successivo alla loro acquisizione da parte degli organi investigativi. Ciò accade quando si procede all'analisi degli strumenti informatici in possesso agli investigatori sequestrati all'indagato e si effettua una ricostruzione *ex post* degli spostamenti del soggetto attraverso sistemi di *computer forensics* e di analisi delle tracce di eventuali sistemi interni di georeferenziazione. Oppure quando si tenta di ricostruire la posizione di un soggetto assunta a ritroso nel tempo attraverso l'analisi dei tabulati e delle celle telefoniche agganciate al sistema. Sul tema S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale*, cit., p. 955 ss.; ID., voce Digital forensic *(investigazioni informatich*e), in *Dig. disc. pen*., Agg. VIII, Utet, 2014, p. 217 s. In altri termini, ritenersi che la simultaneità è caratteristica propria del solo sistema di tracciamento mediante GPS e non anche mediante localizzazione attraverso celle telefoniche. La simultaneità dell'apprensione è anche caratteristica propria del c.d. "tracciamento *AXE*" (dal nome delle centrali Ericsson utilizzate da alcuni operatori di telecomunicazioni) che rappresenta l'evoluzione di quella che, con le vecchie centrali elettromeccaniche, si chiamava «blocco» della chiamata: attraverso il «blocco» – cioè l'arresto degli organi di commutazione su tutta la rete – si poteva materialmente seguire il tracciato della comunicazione all'interno della rete stessa e così individuare la linea del soggetto chiamante. Sul punto e per una differenza con l'acquisizione del tabulato telefonico, C. MARINELLI, voce *Tabulati telefonici (diritto processuale penale)*, in Enc. dir., III, 2010, Giuffrè, p. 111 ss. Sviluppatesi le centrali numeriche, il sistema di individuazione del tracciato, cioè il tracciamento, si è automatizzato ed è diventato seriale, nel senso che non richiede l'isolamento della comunicazione ma avviene automaticamente per ciascuna chiamata. In questo senso F. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito dei tabulati, tracciamenti, intercettazioni, conservazione di dati e dintorni),* in *Cass. pen.,* 2002, f. 12, p. 2214.

velocizzando e facilitando il lavoro degli inquirenti, tali sistemi acuiscono i problemi interpretativi circa il corretto inquadramento dell'attività, dovendo arrendersi di fronte all'impossibilità di sussumere tali attività nelle categorie probatorie tipizzate[148]. Di qui, la scelta di ricomprendere il pedinamento elettronico tra gli atti atipici, regolamentati *ex* art. 189 c.p.p.[149], qualificandola quale «modalità tecnicamente avanzata di pedinamento [e], come tale, rientra nell'ordinaria attività di controllo e accertamento demandata alla p.g. dagli artt. 55, 347 e 370 c.p.p., senza un provvedimento dell'autorità giudiziaria»[150].

Pur ritenendo che il pedinamento elettronico possa pacificamente essere ricompreso nel *genus* dei mezzi di ricerca della prova atipici[151], non si può non evidenziare il maggiore grado di incisività rispetto ai diritti fondamentali allorquando l'attività *de qua* venga condotta mediante il *virus* informatico, dal momento che si consente di rilevare ogni spostamento dell'individuo anche quando entra in luoghi privati, all'interno dei quali non potrebbe estendersi il pedinamento elettronico "tradizionale"[152].

---

[148] Per una ricostruzione della giurisprudenza di legittimità che ha tentato un inquadramento del pedinamento elettronico nell'ambito dei mezzi di ricerca della prova tipici, si rimanda a T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* II ed., cit., p. 443 ss.

[149] Seguono una simile impostazione, Cass., sez. II, 4 aprile 2019, n. 23172, cit.; sez. II, 13 febbraio 2013, n. 21644, cit.; sez. I, 10 gennaio 2012, n. 14529, inedita; Cass., sez. V, 10 marzo 2010, n. 9667cit., p. 1464 ss.; Cass., sez. IV, 29 gennaio 2007, n. 8871, in *Cass. pen*., 2008, p. 1137 ss.; Cass., sez. V, 7 maggio 2004, n. 24715, *ivi*, 2005, p. 3036; Cass., sez. V, 27 febbraio 2002, n. 1630, in *Foro it*., 2002, p. 635 ss. In dottrina T. BENE, *Il pedinamento elettronico: truismi e problemi spinosi,* in AA. VV., *Le indagini atipiche*, I ed., cit., p. 347 ss.; ID., *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* II ed., cit., p. 443 ss.; C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* in *Dir. pen., proc*., 2018, n. 9, p. 1213 s.; D. GENTILE, *Il* Tracking satellitare *mediante GPS: attività atipica di indagine o intercettazione di dati,* in *Dir. pen. proc*., 2010, f. 10, p. 1464 ss.; M. STAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova atipica*, cit., p. 213 ss.

[150] Così Cass., sez. III, 27 febbraio 2015, n. 32699, in *C.E.D. Cass*., n. 264519.

[151] Sembra opportuno precisare che anche il pedinamento elettronico, come tutti i mezzi di ricerca della prova atipici, è sottoposto alle regole di cui all'art. 189 c.p.p. Fuori discussione sembra l'idoneità ad assicurare l'accertamento dei fatti: la geolocalizzazione unisce alla valenza del pedinamento tradizionale la maggiore e più efficace attendibilità fornita dalle nuove tecnologie, consentendo un monitoraggio più sicuro e rapido. Quanto alla tutela della libertà morale della persona, posto che si tratta di uno strumento investigativo occulto e che la sua operatività prescinde da qualsiasi tipo di coercizione e intromissione nella sfera psichica di chi è sottoposto a monitoraggio, sembra impensabile immaginare un nocumento, anche solo potenziale, alla libertà di autodeterminazione o una limitazione delle capacità mnemonico-valutative del soggetto controllato. Infine, il contraddittorio sulle modalità di assunzione deve ritenersi posticipato, in base ad una interpretazione adeguatrice dell'art. 189 c.p.p. che ne consenta l'utilizzo anche con riferimento ai mezzi atipici di ricerca della prova.

[152] L'impiego di tale strumento per finalità investigative è reso possibile, di norma, grazie all'installazione "furtiva" della stazione ricevente il segnale satellitare sull'autovettura del soggetto da monitorare. Come precisato, l'autovettura non è considerato un luogo di privata dimora, difettando di quelle caratteristiche tipiche dei luoghi di privata dimora che consentono l'espletamento, in condizioni di riservatezza, delle più elementari funzioni umane. Cfr. Cass., sez. un., 31 ottobre 2001, n. 42792, in *Foro it*., 2002, f. II, p. 170. Nello stesso anche la giurisprudenza successiva. V. Cass., sez. I, 6 maggio 2008, n. 32851, in *Cass. pen*., 2009, f. 8, p. 2533, per cui l'autovettura non può essere considerata un luogo di privata dimora in quanto quest'ultima è destinata al trasporto «di persone o al trasferimento di oggetti da un luogo ad un altro ed in quanto sfornito dei confort minimi per potervi risiedere stabilmente per un apprezzabile lasso di tempo [...]». Da ultimo, sez. VI, 30 gennaio 2019, n. 23819, in *C.E.D. Cass.,* n. 275994. In dottrina, a favore della

Invero, un'investigazione così congegnata non sembra porre particolari criticità in ordine al rispetto delle prerogative individuali tutelate dagli artt. 13 e 15 Cost.: è da escludere, *ratione obiecti,* l'incidenza dell'art. 15 Cost. a causa della inidoneità del mezzo *de quo* ad interferire con la libertà e la segretezza delle comunicazioni; parimenti, sembra fuorviante immaginare una lesione della libertà fisica e psichica del soggetto monitorato, assolutamente ignaro del controllo subìto.

Non può dirsi, invece, superato il *test* di compatibilità con la previsione di cui all'art. 14 Cost., che interviene a protezione del domicilio informatico su cui il *malware* agisce[153]. Conformemente, anche il diritto al rispetto della vita privata, non potrebbe ritenersi sufficientemente tutelato in un sistema che ammetta una localizzazione satellitare senza limiti[154], non potendosi negare che «l'impiego del sistema di localizzazione g.p.s. realizzi un'interferenza nel diritto alla privatezza […]»[155].

6.2. *SEGUE*: LO *SCREENSHOT* E IL *KEYLOGGING.*

Le diverse forme di *on line surveillance* si concretizzano anche nella decifrazione e nella memorizzazione di tutto ciò che viene digitato sulla tastiera collegata al dispositivo infettato (c.d. *keylogging*), ovvero nella captazione e nella registrazione dell'*output* video del dispositivo bersaglio, permettendo agli inquirenti di apprendere tutta l'attività visualizzata sullo schermo e di memorizzarla mediante fermo immagine (c.d. *screenshot*)[156]. In queste ultime ipotesi, il *malware*, a metà strada tra "copiatore" e

impossibilità di ricondurre l'abitacolo dell'autoveicolo al concetto di domicilio, cfr. P. GIORDANO, *Inapplicabili le garanzie dell'intercettazione al semplice monitoraggio della posizione*, in *Guida dir.,* 2002, f. 23, p. 54, secondo il quale esiste una ontologica ed insuperabile differenza tra un mezzo di trasporto e una privata dimora, poiché quest'ultima «echeggia una struttura abitativa stabile tendenzialmente immobiliare». Sul punto, v. anche T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* II ed., cit., p. 443 ss.

[153] Per una disamina della protezione offerta dall'art. 14 Cost. al domicilio informatico, rinvia a Cap. IV, § ?.

[154]In questo senso L.G. VELANI, *Nuove tecnologie e prova penale: il sistema di individuazione satellitare g.p.s,* in *Giur. it.,* 2003, f. 9, p. 2375, il quale, a ragionar diversamente, avverte anche una potenziale violazione dell'art. 3 Cost., a causa della irragionevole disparità di trattamento tra mezzi di ricerca della prova nominati, per i quali è previsto dal codice di rito il controllo giurisdizionale, e strumenti atipici comunque incidenti, quantomeno, sulla riservatezza.

[155] La Corte Edu, invece, ritiene che il pedinamento satellitare rappresenti un atto che interferisce con l'art. 8 della Convenzione, sia pure in misura meno intensa rispetto ad altri strumenti caratterizzati da maggiore insidiosità; dunque, la legge nazionale deve garantire un'adeguata protezione contro le interferenze arbitrarie nella vita privata, attraverso un "diritto" – ancorché di matrice giurisprudenziale – dettagliato e prevedibile. Corte EDU, sez. V, 2 settembre 2010, *Uzun c. Germania,* n. 35623/05, in *Cass. pen*., 2011, f. 2, p. 395 ss.; sez. V, 8 febbraio 2018, *Ben Faiza c. Francia*, n. 31446/12, in *www. echr.coe.int.* La Corte Suprema americana, invece, ravvisando nel pedinamento satellitare un atto contrario alla Costituzione federale, ritiene necessario il mandato del giudice al fine di acquisire i dati che consentono la geolocalizzazione attraverso le celle telefoniche, pena la violazione del IV Emendamento alla Costituzione federale, salve le ipotesi di eccezionale urgenza e gravità. Cfr. Corte Suprema Americana, 22 giugno 2018, *Carpenter c. United States*, in *www.supremecourt.gov/opinions/17pdf/16–402_h315.pdf*. T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* II ed., cit., p. 444 s.

[156] Sul tema, S. ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante* screen shot, cit., p. 1065 ss.; P. FELICIONI, *Le fattispecie "atipiche" e*

"captatore", non funge soltanto da strumento di copia dal *server* (computer infettato) al *client* (computer in uso alla polizia giudiziaria) ma funziona come se fosse un vero e proprio «specchio dello schermo»[157] del dispositivo infettato, idoneo a riflettere – in tempo pressoché reale – le attività che sono compiute all'interno del sistema, consentendo la graduale acquisizione di ciò che nel tempo si somma al dato già acquisito.

Si tratta, in questi casi, di una vera e propria forma di sorveglianza perpetua che permette di constatare l'evolversi dell'attività criminosa in essere, ma che – allo stesso tempo – incidentalmente coinvolge ogni forma di estrinsecazione dell'attività umana mediante il mezzo informatico, sia essa riconducibile alla vita professionale o a quella privata.

La legittimità degli elementi probatori raccolti discende da una recente impostazione seguita dalla giurisprudenza di legittimità, per cui l'attività di *keylogging* e di *screenshot* rappresenta una modalità esecutiva delle intercettazioni telematiche (art. 266 *bis* c.p.p.)[158].

Al fine di carpire le implicazioni processuali che derivano da una simile scelta, sembra indispensabile interrogarsi sul dato tecnico, ossia sulla peculiare funzione che *malware* esegue sul dispositivo monitorato.

I *keylogger software* consentono di creare dei *files* di *log* contenenti tutto ciò che viene digitato attraverso la tastiera (fisica o virtuale) del dispositivo, da visualizzare in tempo reale o in differita. In alternativa, gli stessi dati possono essere captati durante la loro trasmissione attraverso uno *sniffer*, ovvero *software* che catturano i pacchetti di informazioni in una rete di computer e possono essere utilizzati per monitorare il funzionamento del sistema e/o scoprire nomi utenti e *passwords*[159].

Gli *screenshot*, invece, rappresentano un processo, attivato da un comando remoto, che consente di salvare sotto forma di immagini ciò che viene visualizzato sullo schermo di un computer. A discrezione dell'operatore, ogni "tot" secondi/minuti/ore (è possibile quindi anche variare il tempo) si può impostare uno s*creenshot* che riprende l'attività che appare sullo schermo.

In relazione al primo impiego del *malware*, una recente pronuncia della Suprema Corte chiarisce che «l'uso del *Trojan* […] è [volto] all'acquisizione delle *password* di accesso agli *account* di posta elettronica. Ottenute queste *password*, gli inquirenti […] prendono visione dei messaggi che vengono via via inviati o ricevuti e dei messaggi che vengono salvati nella cartella "bozze"». Di conseguenza, «si è usato il programma informatico […] così come si è da sempre usata la microspia per le intercettazioni»[160].

---

l'impiego processuale, cit., p. 342. Da ultimo L. GIORDANO*, Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. pen*., 2020, f. 4, p. 125 s.

[157] Così C. CONTI-M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in AA. VV., *Le indagini atipiche*, II ed., cit., p. 562.

[158]Cass., sez. IV, 28 giugno 2016, n. 40903, cit.; sez. V, 21 novembre 2017, n. 1822, cit.

[159] Così R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung, cit., p. 697.

[160] Cass., sez. IV, 28 giugno 2016, n. 40903, cit. Nel corso di un'indagine relativa ad un'organizzazione che importava ingenti quantitativi di cocaina dal Sud-America è stata captata la corrispondenza elettronica di diversi imputati. Più specificamente, durante le investigazioni, per mezzo di servizi di pedinamento e osservazione, era stato appurato che gli imputati frequentavano alcuni *internet point* di Roma per accedere ad alcune caselle di posta elettronica attivate presso il *provider* statunitense "*hotmail.com*", con le quali intrattenevano una corrispondenza con i complici sudamericani. I

In sostanza, a parere della Suprema Corte, la funzione di *keylogging* rappresenta solo una modalità alternativa alle tradizionali microspie, idonea a compiere intercettazioni telefoniche (art. 266 *bis* c.p.p.) o ambientali (art. 266, comma 2 c.p.p.)[161].

Sul punto, tuttavia, si avanzano delle riserve. Non sembra, invero, che il *software* sia adoperato per cogliere comunicazioni, quanto piuttosto per individuare ciò che viene digitato sul computer; in questo modo vengono acquisite le *password* che consentono l'accesso agli *account* di posta elettronica ed alle *mail* contenute. Come precisato, «[A]ppare arduo ricomprendere la digitazione sulla tastiera di un computer necessaria per accedere ad una casella di posta elettronica nel concetto di comunicazione»[162], rappresentando un flusso unidirezionale di dati.

Non solo, l'attività acquisitiva delle credenziali di accesso alla casella di posta elettronica, prodromica all'attività intercettiva *strictu sensu* intesa, non così agevolmente può essere sussunta nell'ambito di un'ispezione o una perquisizione di tipo elettronico che ha condotto al sequestro della *password*[163]. Come già più volte chiarito, a fronte di un'incompatibilità ontologica tra il captatore informatico – che determina un monitoraggio occulto e totalizzante del soggetto attenzionato – e i mezzi di ricerca della prova tipici – che si traducono in atti investigativi palesi –, sembra che l'attività *de qua* rappresenti un'indagine "scomposta" nella quale i risultati investigativi tipici sono il frutto di atti di indagine atipici.

---

contatti informatici avvenivano secondo due diverse modalità. In alcuni casi, i messaggi di posta erano normalmente spediti in via telematica; in altri, invece, venivano scritte e-mail che non erano inoltrate al destinatario, ma archiviate nella cartella "bozze". Esse potevano essere lette dai complici che, in possesso di username e password, accedevano successivamente alla casella di posta elettronica. Questo singolare modo di comunicare era impiegato soprattutto per le informazioni più riservate, come quelle che avevano ad oggetto i numeri telefonici "dedicati" allo svolgimento delle singole operazioni di importazione di droga. Le e-mail, in particolare, sono state oggetto di un provvedimento d'intercettazione di flussi telematici in entrata e in uscita dai computer ubicati nei predetti *internet point* ai sensi dell'art. 266 *bis* c.p.p. Le comunicazioni lasciate in "bozza" e quelle che erano state inviate o ricevute in precedenza, ma giacenti nelle diverse cartelle dell'account sono state carpite con un sistema più ingegnoso: gli investigatori si sono procurati le credenziali di accesso controllando a distanza gli imputati tramite un *virus* informatico del tipo *trojan* che, inoculato nei computer, ha permesso di conoscere quanto veniva digitato sulla tastiera; quindi, sono entrati direttamente nelle caselle di posta elettronica, apprendendone il contenuto. Come già anticipato, le *e-mail* pervenute o inviate al destinatario e archiviate nelle cartelle della posta elettronica (cioè "parcheggiate") possono essere oggetto di intercettazione, trattandosi di un flusso di dati già avvenuto ed essendo irrilevante la mancanza del presupposto della loro apprensione contestualmente alla comunicazione. Esulano, invece, dal materiale intercettabile le *e-mail* "bozza", non inviate al destinatario", ma conservate nell'account di posta (o in apposito spazio virtuale come *Dropbox* o *Google Drive*), le quali possono comunque essere acquisite per mezzo di un sequestro di dati informatici. Vedi *supra* § ?. Sul punto, L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* in *Dir. pen. cont.*, 2017, f. 3, p. 177 ss.; M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Dir. pen. cont*., 2018, f. 2, p. 23.

[161] Critico sul punto è M TORRE, *Le intercettazioni a mezzo del c.d. captatore informatico o* "trojan *di Stato*", cit., p. 1671.

[162] Si esprime così L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* in *Dir. pen. cont.*, cit., p. 188.

[163] In questo senso L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico",* cit., p. 189*;* M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* cit., p. 28 s.

Il ragionamento or ora condotto può essere in parte esteso anche all'impiego degli *screenshot* nel procedimento penale.

Di recente, la Corte di cassazione ha previsto che l'acquisizione degli *screenshot* o dei singoli *files* può essere assimilata «alla captazione in tempo reale di flussi informatici transitati sul computer dell'indagato, ovvero di flussi informatici transitati sui dispositivi, rientrante, quest'ultima, nel concetto di intercettazione»[164].

Anche in questo caso l'assimilazione di questa peculiare tecnica investigativa alle intercettazioni telematiche appare eccessivamente semplicistica[165]. Pur potendo captare

[164] Cass., sez. V, 20 ottobre 2017, n. 48370, cit. Per comprendere appieno l'*iter* logico seguito dalla quinta sezione della Corte di cassazione, si ritiene opportuno ripercorrere brevemente la vicenda giudiziaria de qua, che prende le mosse da un ricorso cautelare della difesa degli indagati. Il Tribunale del riesame di Roma, con l'ordinanza impugnata, conferma il provvedimento applicativo della custodia cautelare in carcere per i due imputati, perseguiti per i reati di cui agli artt. 494, 615 *ter*, 617 *quater* e *quinquies* c.p., per avere provocato un accesso abusivo alla casella di posta elettronica in uso ad uno studio legale, da dove, sostituendosi al titolare, ponevano in essere, inviando all'ENAV un messaggio di posta contenente in allegato un *virus* informatico ben mimetizzato, atti idonei all'accesso abusivo al relativo sistema informatico contenente dati relativi alla sicurezza pubblica nel settore dell'aviazione civile e all'intercettazione delle comunicazioni telematiche al suo interno. In più, i due imputati vengono accusati dei reati di cui agli artt. 615 *ter*, 615 *quater* e 617 *quinquies* c.p., per aver fatto abusivamente accesso o aver tentato di fare accesso a caselle di posta elettronica appartenenti a professionisti del settore giuridico ed economico, ad autorità politiche e militari di importanza strategica, nonché utilizzati dallo Stato e da altri enti pubblici, allo scopo, mediante installazione del predetto virus informatico, di acquisire notizie riservate, dati personali e dati sensibili. In seguito alla denuncia del responsabile della sicurezza dell'ENAV (che - insospettito - ha inviato ad una ditta specializzata l'analisi tecnica del *malware*), l'a.g. procede ad attivare sia intercettazioni telefoniche sia intercettazioni telematiche "classiche" riuscendo, poi, seppur con molte difficoltà e per pochissimi giorni, ad inoculare il captatore informatico sul personal computer dell'indagato. In altri termini, l'indagine si compone in parte di intercettazioni telematiche "tradizionali", eseguite per diverse settimane al fine di captare il flusso di comunicazioni informatiche "in chiaro" prodotte attraverso il personal computer dell'indagato, finanche sui server allocati negli Stati Uniti (dotati anch'essi, come il computer dell'indagato, di un sistema di cifratura). Onde bypassare tale ostacolo, l'a.g. sceglie, poi, di utilizzare le cc.dd. intercettazioni telematiche "attive", con il captatore informatico, inoculando il *malware* per una manciata di giorni. Lo fa attraverso un decreto di intercettazione e di intercettazione telematica, autorizzando altresì le captazioni di intercettazioni audio tra presenti e i cc.dd. *screen shot*. Per una ricostruzione della vicenda, S. ATERNO, *La Cassazione, alle prese con il captatore informatico,* cit., p. 1065 ss. Più di recente, la Suprema Corte afferma che «i messaggi *WhatsApp* così come gli sms conservati nella memoria di un apparecchio cellulare hanno natura di documenti ai sensi dell'art. 234 c.p.p., di tal che la relativa attività acquisitiva non soggiace alle regole stabilite per la corrispondenza, nè tantomeno alla disciplina delle intercettazioni telefoniche, con l'ulteriore conseguenza che detti testi devono ritenersi legittimamente acquisiti ed utilizzabili ai fini della decisione ove ottenuti mediante riproduzione fotografica a cura degli inquirenti». Gli sms, le conversazioni *Whatsapp,* i messaggi di posta elettronica "scaricati" e/o conservati nella memoria dell'apparecchio cellulare possono essere, dunque, legittimamente acquisiti in giudizio con una qualunque modalità atta alla raccolta del dato, inclusa la riproduzione fotografica". Cass., sez. V, 21 novembre 2017, n. 1822, cit. Nell'occasione, la Corte chiarisce che lo *screenshot* eseguito dagli inquirenti ha valore legale differente rispetto a quello eseguito dalla parte. I primi, infatti, sono pubblici ufficiali e hanno il potere di certificare la corrispondenza della copia all'originale, potere che, invece, il privato non ha. In conclusione, lo *screenshot* prodotto in giudizio dalla parte ha valore documentale solo se non viene contestato dalla controparte. Sul punto, i giudici della Corte di Cassazione hanno ribadito più volte che la contestazione della prova fotografica è possibile solo se supportata da fondati motivi (es. qualora manca l'indicazione del mittente o la data di spedizione del messaggio.

[165] Secondo S. ATERNO *La Cassazione, alle prese con il captatore informatico,* cit., p. 1069, per cui

anche un flusso comunicativo, «[N]non si tratta di intercettazioni ambientali con l'uso del microfono; non si tratta di captare da remoto tutti i *files* e contenuti del supporto, bensì […] di fare una "foto" di ciò che appare a video ovvero di ciò che l'utente del telefono sta facendo»[166]. In presenza, comunque, di un decreto di intercettazione telematica con l'uso del *Trojan* su questa modalità *screenshot* si acquisisce in chiaro (parte di) ciò che è cifrato e che appare sullo schermo dello *smartphone* o di un *personal computer* nel momento in cui l'utente utilizza lo strumento informatico: con delle vere e proprie fotografie dello schermo effettuate dal *software* posto all'interno dello *smartphone/pc*, il *malware* acquisisce - o può comunque acquisire - le informazioni più svariate sia dei contenuti comunicativi sia di quelli non comunicativi, nonché quelle che esulano dall'interesse investigativo concretamente perseguito dagli inquirenti[167].

Dunque, seppur il *trend* seguito dalla giurisprudenza sia volto a legittimare l'impiego del captatore a prescindere dalla funzione utilizzata, l'attività svolta con il captatore informatico realizza qualcosa di «trasversale»[168] rispetto al panorama giuridico esistente; attività che solo in parte, con interpretazioni estensive ai limiti della forzatura, è possibile farle rientrare nel concetto di intercettazione telematica *ex* art. 266 *bis* c.p.p.[169], dovendo prediligere l'impostazione per cui l'attività *de qua* possa essere assimilate alle perquisizioni *online*, avendo ad oggetto il monitoraggio occulto dei "movimenti" in rete atto all'acquisizione di informazioni – anche e molto spesso– non comunicative.

Non si può tuttavia negare che l'acquisizione di dati informatici condotta mediante l'impiego del *malware* rappresenti qualcosa di più e di diverso rispetto un'investigazione atipica "tradizionale": controllare in modo occulto e continuativo ciò che una persona digita sulla tastiera e ciò che visualizza sullo schermo del proprio *device*, non solo mette a repentaglio la riservatezza genericamente intesa del soggetto monitorato ma qualcosa di molto più profondo e intimo. Il dispositivo elettronico, soprattutto se mobile, rappresenta «un'appendice della persona, in grado si rivelarne i segreti più nascosti ed inconfessabili»[170]. Di qui, può sostenersi che la videoregistrazione della successione della schermata di un computer e lo spionaggio della digitazione della tastiera rappresentano attività che giungono ad un livello di invasività tale da «aggredire il foro interno di una persona»[171], riferibile a quel complesso di diritti espressamente tutelato dagli artt. 14 e 15 Cost., anche con precipui riferimento alla protezione della proiezione dell'individuo

---

«[S]se con lo *screen shot* si riesce a captare una conversazione via chat o una comunicazione tra due soggetti in tempo reale ovvero in corso di svolgimento non si ravvedono differenze con una telecamera o una macchina fotografica che riprende il contenuto comunicativo (qualsiasi) di un soggetto che dialoga o che scrive con un altro soggetto situato anche fuori dal luogo in cui è ripreso». Di qui, sarebbe più logico sussumere tali attività nell'ambito delle intercettazioni ambientali domiciliari condotte mediante il supporto di strumenti atipici.

[166] S. ATERNO, *La Cassazione, alle prese con il captatore informatico,* cit., p. 1069.

[167] Come sostenuto, tali attività potrebbero essere definite come ispezioni *on-line*. In questo senso, P. FELICIONI, *L'acquisizione da remoto,* cit., p. 124.

[168] Cfr. C. CONTI-M. TORRE, *Spionaggio digitale nell'ambito dei* social network, cit., p. 562.

[169] In effetti, si potrebbe propendere per un simile inquadramento solo nel caso in cui l'attività abbia ad oggetto la captazione in tempo reale di comunicazioni.

[170] Così S. RODOTÁ, *Una scommessa impegnativa sul terreno dei nuovi diritti, Discorso del presidente del Garante per la protezione dei dati personali tenuto l'8 maggio 2001alla presentazione della Relazione per il 2001,* 15 maggio 2002, in *www.privacy.it*

[171] C. CONTI-M. TORRE, *Spionaggio digitale,* cit., p. 564.

nell'etere digitale, presidiando la sua soggettività in rapporto a qualunque dato o attività svolta nell'ambito di un sistema informatico e della rete.

6.3 *SEGUE*: LE VIDEORIPRESE INVESTIGATIVE

Le videoriprese investigative eseguite dalla p.g. mediante l'attivazione della videocamera del dispositivo su cui il *malware* è inoculato, occupano una posizione di rilievo tra le attività di *online surveillance*[172], offrendo al processo elementi assai utili all'accertamento dei fatti che interessa provare[173].

[172] Come precisa parte della dottrina le videoriprese investigative possono rappresentare «a tutti gli effetti un'attività investigativa a sé». In questo senso, A. SIGNORATO, *Le indagini digitali,* cit., p. 272.
[173] Sul tema, v. E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 533 ss.; S. BELTRANI, *Le videoriprese? Sono una prova atipica ma le Sezioni unite non sciolgono il nodo*, in *Dir. e giust*., 2006, p. 34 ss.; V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede una sistemazione legislativa,* in *Proc. pen. giust.,* 2019, f. 2, p. 338 ss.G. BORRELLI, *Riprese visive filmate nel bagno di un pubblico esercizio e garanzie costituzionali,* in *Cass. pen*., 2001, f. 12, p. 2446 e ss.; C. CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati",* in *Dir. pen. proc*., 2006, n. 11, p. 1347 ss.; M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen*., 2006, f. 12, p. 3950; C. IASEVOLI, L*a nomofilachia "creatrice" in materia di videoriprese,* in AA. VV., *L'intercettazione di comunicazioni*, cit., p. 285 ss.; F. RUGGIERI, *Riprese visive e inammissibilità della prova,* in *Cass. pen*., 2006, f. 12, p. 3945; N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni,* in AA. VV., *Le indagini atipiche*, II ed., cit., p. 161 ss.

Nonostante l'importanza di tali atti di indagine, il legislatore non ha provveduto[174] (e nemmeno provvede[175]) a disciplinare la materia che, di conseguenza, è il risultato di una lenta stratificazione giurisprudenziale[176] e di un focoso dibattito dottrinale[177].

---

[174] Sottolineano la carenza di una disciplina normativa, A. SCALFATI, *Orientamenti in tema di videoriprese*, in *Proc. pen. giust.,* 2011, p. 1; C. IASEVOLI, *La nomofilachia "creatrice"*, cit., p. 285 ss.;

[175] Come noto, il legislatore del 2017 non norma altre funzioni se non quella dell'attivazione del microfono del dispositivo su cui il *malware* è inoculato per condurre intercettazioni di conversazioni e comunicazioni tra presenti. Sul punto si rinvia a § 1.

[176] La prima decisione della giurisprudenza di legittimità sul tema della captazione di immagini con una videocamera collocata all'interno di un luogo di privata dimora risolve la questione adottando un criterio discretivo che viene mantenuto fermo dalla giurisprudenza successiva. In quell'occasione la Corte distingue tra videoriprese che hanno ad oggetto comportamenti comunicativi e quelli che non sono diretti all'intenzionale scambio di messaggi. Nel primo caso, secondo la Corte, si è in presenza di una forma peculiare di intercettazione ambientale e come tale pienamente utilizzabile *ex* art. 266, comma 2 c.p.p. Qualora, invece, la captazione abbia ad oggetto comportamenti non comunicativi, allora la disciplina da applicare è quella dell'art. 189 c.p.p., ritenute inutilizzabili perché acquisite in violazione dell'art. 14 Cost. In questo senso Cass., sez. VI, 10 novembre 1997, n. 4379, in *Cass. pen*., 1999, f. 9, p. 1188, con nota di A. CAMON, *Le riprese visive come mezzo di indagine: spunti per ina riflessione sulle prove "incostituzionali.* Cfr. anche C. MARINELLI, *Le "intercettazioni di immagini" tra questioni interpretative e limiti costituzionali,* in *Dir. pen. proc*., 1998, f. 10, p. 1265 ss. Dopo una breve battuta d'arresto in cui la Corte di legittimità vieta *tout court* le videoriprese nel domicilio (Cass., sez. IV, 16 marzo 200, n. 562, in C*ass. pen.,* 2001, f. 12, p. 2434, con nota di G. BORRELLI, *Riprese filmate nel bagno di un pubblico esercizio e garanzie costituzionali*. Sul tema anche L. FILIPPI, L'home watching: *documento, prova atipica o prova incostituzionale?,* cit., p. 87 s.), la questione viene sottoposta al vaglio del Giudice delle leggi che, di fatto, riprende e rielabora la distinzione già operata dalla Corte di Cassazione nel 1997 tra comportamenti comunicativi e non comunicativi, sancendo che la videoripresa avente ad oggetto comunicazioni, soggiace alla disciplina di cui all'art. 266, comma 2 c.p.p. mentre quelle di sole immagini si configura quale prova atipica vietata nel domicilio. Cfr. Corte cost., 24 aprile 2002, n. 135, in *Giur. cost.,* 2002, p. 1062, con nota di A. PACE*, Le videoregistrazioni "ambientali" tra gli artt. 14 e 15 Cost.* e di F.S. MARINI, *La costituzionalità delle riprese visive nel domicilio: ispezione o libertà "sotto-ordinata"?*. A commento della decisione, v. altresì R. BRICCHETTI, *Spetta al legislatore regolamentare le riprese di tipo non comunicativo,* in *Giuda dir.,* 2003, f. 20, p. 73 s.; F. CAPRIOLI, *Riprese visive nel domicilio e intercettazione "per immagini",* in *Giur. cost.,* 2002, p. 2176 ss. Le successive pronunce della giurisprudenza di legittimità, pur tenendo come punto fermo il *dictum* della Corte costituzionale (Cass., sez. I, 29 gennaio 2003, n. 16965, in *Cass. pen.,* 2004, f. 9, p. 1304. *Contra*, Cass., sez. IV, 8 giugno 2003, n. 44484, *ivi*, 2004, f. 12, p. 3280, con nota dii L. SAPONARO, *Sulla* vexata quaestio *della natura delle videoregistrazioni*) accoglievano una nozione assai restrittiva di domicilio, in modo da rendere ammissibili le videoriprese di mere immagini anche in luoghi in cui l'aspettativa di riservatezza risultava assai maggiore rispetto ai luoghi pubblici. Cfr. Cass., sez. VI, 12 febbraio 2003, n. 6962, in *C.E.D. Cass*., n.223733; sez. VI, 10 gennaio 2003, n. 3442, in *Cass. pen.,* 2004, f. 6, p. 1305, con nota critica di D. ZIGNANI, *Una discutibile pronuncia in tema di prove illegittimamente carpite nel domicilio*. Di qui, nel 2006 la Suprema corte, pur recependo l'orientamento della Consulta del 2002, amplia la portata del concetto di domicilio: confermando la distinzione già prospettata tra immagini non comunicative e non, Corte ha prospettato tre differenti discipline a seconda del luogo in cui la captazione è effettuata. Nei luoghi domiciliari le videoriprese di immagini non comunicative sono senz'altro vietate, a pena di inutilizzabilità Nei luoghi riservati, in cui manca la stabilità dello *ius excudendi alios* (esistendo il diritto solo se l soggetto è presente sul luogo) ma sussiste «un' aspettativa di riservatezza maggiore rispetto ai luoghi pubblici», tutelato *ex* art. 2 Cost., sono consentite le videoriprese di immagini non comunicative, purché disposte con provvedimento dell' a.g., fornito di congrua motivazione. Nei luoghi pubblici, le videoriprese possono essere effettuate dalla p.g. nel corso delle indagini preliminari, anche di propria iniziativa. In questi ultimi due casi le videoriprese possono essere utilizzate come prova atipica. Così Cass., sez. un., 28 luglio 2006, n. 26795, cit. A commento della pronuncia v. S. BELTRANI, Le videoriprese? Sono una prova atipica ma le Sezioni unite non sciolgono il nodo, cit., p. 34 ss.; A. CAMON, *Le Sezioni unite sulla*

Allo stato dell'arte, può dirsi che l'istituto assuma sembianze diverse a seconda dell'oggetto captato e, dunque, i risultati investigativi appresi seguono discipline diversificate con altrettanti regimi di utilizzabilità a seconda della qualifica assunta.

In particolare, nel caso in cui l'oggetto della videoripresa sia rappresentato da sole immagini (ovvero da comportamenti non comunicativi, quali, ad esempio, i movimenti dei soggetti in un ambiente), il dato probatorio acquisito soggiace alla disciplina di cui all'art. 189 c.p.p.; viceversa, allorquando vengano appresi anche contenuti comunicativi (ad esempio, due persona che dialogano tra loro a gesti), tale attività è inquadrabile nel *genus* delle intercettazioni ambientali, *ex* art. 266, comma 2 c.p.p.

In questa prospettiva, le videoriprese effettuate in un luogo pubblico[178], sono legittime e pienamente utilizzabili anche in assenza di un decreto autorizzativo, purchè le modalità di assunzione previste dall'art. 189 c.p.p. siano state oggetto di contraddittorio, sia pure posticipato.

Nei luoghi "riservati"[179], soggetti alla tutela della *privacy* ma non a quella offerta al domicilio, la videoripresa deve essere autorizzata con apposito decreto, desumendo tale necessità dall'art. 2 Cost.

Infine, nei luoghi domiciliari[180] gli elementi di prova acquisiti *ex* art. 189 c.p.p., sono inutilizzabili, in quanto basati su un'attività che la legge vieta.

---

videoregistrazione come prova penale: qualche chiarimento e alcuni dubbi nuovi, in *Riv. it. dir. proc. pen.,* 2006, f. 6, p. 1550; A. CISTERNA, *I filmati nel* privè *di un locale pubblico possono rientrare tra le prove atipiche,* in *Guida dir.,* 2006, f. 33, p. 60 ss.; C. CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni unite elaborano la categoria dei luoghi "riservati",* cit., p. 1347; M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni unite,* cit., p. 3950; F. RUGGIERI, *Riprese visive,* cit., p. 3945.

[177] Ricostruiscono efficacemente i termini del dibattito dottrinale sviluppatosi in materia, C. IASEVOLI, *La nomofilachia "creatrice" in materia di videoriprese,* cit., p. 285 ss.; C. MARINELLI, *Intercettazioni processuali,* cit., p.159 ss.; G. TABASCO, *Prove non disciplinate dalla legge nel processo penale*, cit., p.142 e s.; N. TRIGGIANI, *Le videoriprese investigative*, cit., p. 161.

[178] Di recente la giurisprudenza ha ridefinito i termini dei "luoghi pubblici" e di quelli "aperti al pubblico". Cfr. Cass., sez. VI, 21 novembre 2017, n. 595, in *C.E.D. Cass.,* n. 271763, secondo cui «l'area antistante un condominio, recintata ma priva di cancello, costituisce luogo aperto al pubblico, in quanto consente l'accesso ad una categoria indistinta di persone a non solo ai condomini». Così come sono considerati tali «la cella e gli ambienti penitenziari […] non essendo nel "possesso" dei detenuti, ai quali non compete alcuno "*ius excludendi alios*"; tali ambienti, infatti, si trovano nella piena e completa disponibilità dell'amministrazione penitenziaria, che ne può fare uso in ogni momento per qualsiasi esigenza d'istituto». Cass., sez. VI, 15 maggio 2018, n. 26028, in *C.E.D. Cass.,* n.273417.

[179] Nei luoghi riservati manca la stabilità dello *ius excudendi alios* (esistendo il diritto solo se l soggetto è presente sul luogo) ma sussiste un'aspettativa di riservatezza maggiore rispetto ai luoghi pubblici». Cass., sez. un., 28 luglio 2006, n. 26795, cit. Nello stesso senso sez. V, 3 marzo 2009, n. 11522, in *C.E.D. Cass.,* n. 244199.

[180] In base all'evoluzione giurisprudenziale, può dirsi che i luoghi "domiciliari" sono quei luoghi in cui il titolare possiede uno *ius excludendi alios* stabile, ovvero azionabile anche quando il soggetto non sia fisicamente presente. Corte cost., 16 maggio 2008, n. 149, in *Giur. cost.,* 2008, p. 1825, con commento di F. CAPRIOLI, *Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva.* Tale profilo era già emerso nella giurisprudenza di legittimità. Come precisato, il carattere di "stabilità" del diritto risulta, ai fini della determinazione del concetto di domicilio, assolutamente necessario (Cass., sez. IV, 20 giugno 2018, n. 32245, in *C.E.D. Cass*., n. 273458). Rientrano, pertanto, nella nozione di domicilio solo i luoghi che assolvono in concreto alla finalità di proteggere la vita privata del loro possessore, durante lo svolgimento delle sue attività professionali, di svago, di alimentazione, di riposo. In questo senso, G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali*

La fragilità di una disciplina così congegnata – non fondata su basi normative stabili ma su interpretazioni giurisprudenziali e dottrinali peraltro ondivaghe – determina effetti perniciosi sui limiti stessi del divieto introdotto, finendo per legittimare tutte quelle attività investigative dai contorni più sfumati, al limite tra acquisizione di immagini aventi ad oggetto comportamenti comunicativi e non[181], in luoghi non perfettamente inquadrabili nelle categorie sopra indicate[182]; come sapientemente osservato, «residuano "zone grigie", dove la prassi è incline ad aperture in chiave autoritaristica»[183].

Le perplessità or ora evidenziate si acuiscono nel caso delle investigazioni mediante *Trojan.* Utilizzando un *malware* per attivare la *webcam* del dispositivo, infatti, risulta estremamente difficile prevedere sia l'esatto luogo in cui è situato (considerato il carattere

contro la pubblica amministrazione, in AA. VV., *Le nuove intercettazioni*, cit., p. 139 s. Detto in altri termini, affinché scatti la protezione prevista da tale articolo, non basta che un comportamento venga tenuto in un luogo di privata dimora, in quanto occorre che esso sia in concreto riservato, e, cioè non possa in concreto essere liberamente osservato dagli estranei, senza ricorrere a particolari accorgimenti. Sulla scia della Consulta anche la giurisprudenza di legittimità. Solo per citare alcuni esempi, Cass., sez. II, 24 ottobre 2014, n. 46786, in *C.E.D. Cass*., n. 261053, secondo cui «sono legittime e pienamente utilizzabili senza alcuna autorizzazione dell'autorità giudiziaria le videoriprese, eseguite da privati, mediante telecamera esterna installata sulla loro proprietà, che consentono di captare ciò che accade nell'ingresso, nel cortile e sui balconi del domicilio di terzi, i quali, rispetto alle azioni che *ivi* si compiono, non possono vantare alcuna pretesa al rispetto della riservatezza, trattandosi di luoghi, che, pur essendo di privata dimora, sono liberamente visibili dall'esterno, senza ricorrere a particolari accorgimenti»; sez. I, 25 ottobre 2006, n. 37530, in *Cass. pen.,* 2007, f. 12, p. 4643, con nota di C. MARINELLI, *Le videoriprese investigative in luoghi esposti al pubblico: verso la progressiva emersione dei criteri di qualificazione degli ambiti spaziali soggetti alle operazioni*; sez. V, 17 novembre 2015, n. 11419, in *Foro it.,* 2017, f. 2, p. 139, con nota di D. LAZZARI, *Videoriprese: il confine tra esigenze investigative e garanzie costituzionali*, per cui «sono utilizzabili ai fini probatori, pur in assenza di un provvedimento motivato di autorizzazione del giudice o del p.m., le videoriprese compiute dalla p.g. in un luogo riservato nel caso in cui lo stesso abbia caratteristiche tali da essere facilmente visibili dai terzi». Seguendo un simile filone interpretativo, può sostenersi che non sono considerati domicilio, le stanze di un ospedale (sez. V, 11 ottobre 2018, n. 5300, in *C.E.D. Cass.,* n. 27592) o le celle carcerari (sez. VI, 15 maggio 2018, n. 26028, *ivi*, n. 273417), il pianerottolo di un'abitazione privata (sez. 5, 30 maggio 2017, n. 34151, *ivi,* n. 270679), il *box* cassa di un'autorimessa (sez. V, 17 novembre 2015, n. 11419, in *Cass. pen*., 2017, f. 2, p. 722 ss., con nota di C. RIZZO, *Videoregistrazioni domiciliari e l'incerta distinzione tra comportamenti comunicativi e non)*. Per una ricostruzione della giurisprudenza espressasi sul punto, cfr. V. BONINI, *Videoriprese investigative e tutela della riservatezza,* cit., p. 336 ss. La delicata *quaestio* sembra aver trovato una stabilità ermeneutica grazie al recente apporto delle sezioni unite che accoglie un'interpretazione maggiormente restrittiva alla nozione *de qua*. Cfr. Cass., sez. un., 23 marzo 2017, n. 31345, in *Dir. pen. cont*., 2017, f. 7/8, con nota di S. BERARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624* bis *c.p.,* secondo cui «rientrano nella nozione di privata dimora di cui all'art. 624 *bis* c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare». Per una ricostruzione storica della nozione di privata dimora v. L. FILIPPI, sub *art. 226*, cit., p. 2541 ss.

[181] Sottolinea A. CAMON, voce *Captazione di immagini (dir. proc. pen.)*, in *Enc. dir*., Annali VI, , Giuffrè, 2013, p. 143 s., che «la distinzione tra comportamenti comunicativi e non ha qualcosa di artificioso […], in quanto spezza in due uno strumento investigativo in realtà unitario quanto a tipologia, natura, grado e modalità di compressione del bene tutelato». Più di recente, C. RIZZO, *Videoregistrazioni domiciliari,* cit., p. 722 ss.

[182] Tali riflessioni sono svolte da N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, cit., p. 183.

[183] L'espressione appartiene a A. SCALFATI, *Orientamenti in tema di videoriprese*, cit., p. 93.

di *iper*-trasportabilità di talune tecnologie) sia il tipo di comportamento, comunicativo o semplice, oggetto di captazione.

In altri termini, l'uso della *webcam* spinge l'investigazione tramite videoriprese verso livelli di incertezza operativa difficilmente accettabili: non solo non è dato sapere se l'attivazione della videocamera dia luogo ad un'intercettazione – dal momento che non si può prevedere si stiano tenendo o meno delle conversazioni - ma, non potendo sapere il momento in cui si «apre l'occhio dell'inquirente»[184], neppure è possibile pronosticare se questi realizzerà un'intrusione vietata o piuttosto se si avvarrà di un mezzo d'indagine atipico.

Queste incertezze «trasformano una risorsa investigativa indiscutibilmente formidabile in uno strumento giuridico pressappoco inservibile»[185].

Se così stanno le cose, l'attivazione da remoto della videocamera di cui è dotato il dispositivo mobile consentirebbe di effettuare videoriprese di comportamenti non comunicativi anche nell'ambito domiciliare che, come anticipato, risultano essere inutilizzabili, in quanto acquisite illecitamente[186]. Ma l'inutilizzabilità costituisce una risposta inadeguata alla violazione dei diritti fondamentali, i cui esiti non verrebbero così scongiurati[187].

Non solo. L'erosione dei confini del divieto, combinato all'itineranza ontologica del *virus* informatico, potrebbe determinare l'apprensione di una mole di dati che non sempre sono esclusi dagli esiti procedimentali. A ben guardare, infatti, non sono mancate decisioni della giurisprudenza di legittimità in cui si è affermata la piena utilizzabilità delle videoriprese di comportamenti materiali realizzate in ambito domiciliare, allorquando tale captazione fosse avvenuta "incidentalmente", nel corso di un'attività di un'indagine volta, in base ad una valutazione *ex ante*, alla registrazione di comportamenti comunicativi e, dunque, autorizzata ai sensi dell'art. 266, comma 2 c.p.p.[188].

---

[184] Così F. PALMIROTTO, *Le indagini informatiche e la tutela della riservatezza*, in *www.legislazionepenale.eu*, 1 luglio 2019.

[185] F.B. MORELLI, *Videoriprese mediante* la webcam *di un computer illecitamente sottratto e tutela del domicilio,* in *Dir. pen. proc*., 2013, f. 3, p. 475.

[186] Come precisato dalla giurisprudenza di legittimità, «[L]le videoriprese effettuate "da remoto", mediante l'attivazione attraverso un virus informatico della telecamera di un apparecchio telefonico *smartphone*, possono ritenersi legittime quali prove atipiche ai sensi dell'art. 189 c.p.p. salvo che siano effettuate all'interno di luoghi di privata dimora, e ferma la necessità di autorizzazione motivata dall'A.G. per le riprese che, pur non comportando una intrusione domiciliare, violino la riservatezza personale». Così Cass., sez. VI, 26 maggio 2015, n. 27100, in *Guida dir*., 2015, f. 41, p. 83 s.

[187] Sul tema, si rinvia a Cap. III, § ?

[188] In questo senso, Cass., sez. IV, 20 marzo 2008, FERA ANDALI, in *Guida dir*., 2008, f. 18, p. 97. *Contra*, sez. VI, 8 novembre 2012, n. 1287, in *Dir. pen. proc*., 2013, f. 11, p. 1336, con nota di A. INNOCENTI, *La videoregistrazione domiciliare di comportamenti comunicativi nella previsione e non comunicativi nei risultati*, per cui «[S]sono inutilizzabili le riprese video, pur se autorizzate dal Gip, di comportamenti non comunicativi, eseguite all'interno del domicilio anche se esse abbiano registrato attività direttamente criminose». Sul punto, v. anche la ricostruzione offerta da N. TRIGGIANI, *Le videoriprese investigative e l'uso dei droni*, cit., p. 184

7. IL CAPTATORE INFORMATICO TRA ATIPICITÀ, IRRITUALITÀ E INCOSTITUZIONALITÀ

Dalla disamina delle differenti *species* di investigazioni esperibili mediante l'impiego del captatore informatico, emerge che esse, ad eccezione di rare ipotesi per cui il *Trojan* si limiti ad apprendere i flussi comunicativi "in transito", appaiono difficilmente riconducibili al catalogo degli atti noti, in quanto le caratteristiche che potrebbero assimilarle a questi ultimi risultano sempre cedevoli rispetto ai profili differenziali determinati dalle peculiarità tecniche dello strumento impiegato.

Di qui, per attribuire al dato investigativo così acquisito valore di prova, ne è stata suggerita la sussunzione nella nebulosa categoria dei mezzi di ricerca della prova atipici e, più concretamente, nell'ambito delle perquisizioni *online*, con cui tali attività condividono la segretezza e l'incisività nella sfera privata del monitorato.

Come noto, tuttavia, l'atipicità non può giustificare la legittimità di qualsivoglia atto investigativo, dal momento che anche questa categoria probatoria è sottoposta al vaglio di compatibilità costituzionale[189]: «tali valori, infatti, […] sono chiamati a fungere da riferimento diretto e limite invalicabile, superato il quale le risultanze probatorie sarebbero incostituzionali»[190].

In altri termini, esiste uno specifico ambito nel quale la legge non ammette prove e investigazioni "atipiche"[191], allorquando le stesse possono ledere i tre diritti che il titolo

---

[189] F. SORRENTINO, *Lezioni sul principio di legalità*, Giappichelli, 2007, p. 3, per cui «per le pubbliche autorità, la legge rappresenta il titolo ed il fondamento per l'esercizio dei loro poteri autoritativi […] condizione ineliminabile del loro agire».

[190] Così P. MAGGIO, *La registrazione occulta curata da una persona presente al colloquio*, in AA. VV., *Le indagini atipiche*, II ed., cit., p. 111 s. Nello stesso senso, A. CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali,* in *Cass. pen*., 1999, p. 1200 ss.; P. TONINI-C. CONTI, *Il diritto delle prove penali,* II ed., cit., p. 201; L. PARLATO, *Problemi insoluti*, cit., p. 313. Con tale sintagma la dottrina è solita indicare quegli elementi di prova che vengono acquisiti con modalità non disciplinate dal codice di rito e lesive dei diritti fondamentali dell'individuo costituzionalmente tutelati. Per tutti, v. V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale*, in *Giur. cost.,* 1973, p. 341.

[191] In proposito si sono formati orientamenti differenti. Da un lato, si prospetta una interpretazione estensiva dell'espressione «divieti stabiliti dalla legge» prevista dall'art. 191, comma 1 c.p.p. in tema di inutilizzabilità. In base a questa tesi, nel concetto di "legge" rientra anche la Carta fondamentale. L.P. COMOGLIO, *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen*., 1996, f. 10, p.1548; L. FILIPPI, *Ascolto e trascrizione di telefonate all'inquisito: sommarie informazioni o prova incostituzionale?, ivi*, 2001,f. 9, p. 1395; F.M. GRIFANTINI, voce *Inutilizzabilità,* in *Dig. disc. pen*., VII, Utet, 1993, p. 249. Vi è chi sostiene che a tale conclusione si può pervenire attraverso una interpretazione costituzionalmente orientata dell'art. 191 c.p.p. nella parte in cui menziona i divieti stabiliti dalla legge. In questo senso A. CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove incostituzionali,* in *Cass. pen*., 1999, p. 1200 ss. Da un altro lato, vi è chi ritiene che la Carta fondamentale non possa costituire fonte diretta di divieti in assenza di una norma legislativa interposta. Pertanto - si afferma - l'assenza di un divieto probatorio espresso nel codice di procedura penale impedisce di sanzionare l'atto acquisitivo: de iure condito, l'elemento acquisito è utilizzabile. Cfr. F. CORDERO, *Procedura penale*, Giuffrè, VII ed., 2003, p. 848; N. GALANTINI, voce *Inutilizzabilità (dir. proc. pen*.), in *Enc. dir.,* Agg. I, 1997, p. 700 ss. Invero, il primo orientamento trova conferme in diverse pronunce della Corte costituzionale e della giurisprudenza di legittimità. Corte cost., 6 aprile 1973, n. 34 in *Giur. cost*., 1973, p. 341; 11 marzo 1993, n. 81, *ivi*, 1993, p. 731; 18 giugno 1998, n. 229, in *Cass. pen*., 1998, p. 2847. Nella giurisprudenza di legittimità, Cass., sez. un., 23 febbraio 2000, n. 6, in *Cass. pen*., 2000, f. 12, p. 2594; sez. Un., 13 luglio 1998, n. 21, *ivi,* 1999, f. 2, p. 465; Sez. Un., 16 maggio 1996, n. 5021,

primo della parte prima della Costituzione italiana definisce "inviolabili": il diritto alla libertà personale (art. 13 Cost.), il diritto all'intimità domiciliare (art. 14 Cost.) e il diritto alla libertà e alla segretezza delle comunicazioni (art. 15 Cost.). Tutte le attività probatorie che comportano una violazione di questi tre fondamentali diritti dell'individuo devono essere previste tassativamente dalla legge. Gli artt. 13, 14 e 15 della Costituzione italiana stabiliscono infatti che non è consentita alcuna limitazione di tali diritti – neppure nel corso di un'indagine o di un processo penale – se non per atto motivato dell'autorità giudiziaria (riserva di giurisdizione) e «nei casi e modi previsti dalla legge», ovvero «con le garanzie stabilite dalla legge» (riserva di legge)[192].

Analogamente, l'art. 8 della Convenzione Europea dei diritti dell'uomo impone che sia «prevista dalla legge» ogni intrusione dell'autorità pubblica non solo nell'intimità della corrispondenza e del domicilio, ma in genere nella "vita privata" dell'individuo[193].

Accolta questa premessa, occorre dunque chiedersi se le investigazioni penali effettuate con l'ausilio dei *virus Trojan* siano o meno lesive dei diritti individuali fondamentali: se la risposta è negativa, nulla vieta, in linea di principio, di ritenere ammissibili le investigazioni di cui si tratta, anche in difetto di una specifica base legale. Se la risposta è positiva, posto che tali attività non possono essere sussunte nell'ambito di fattispecie investigative e probatorie già regolate della legge, allora la diagnosi di ammissibilità non potrà che essere sfavorevole.

Non si può negare che le attività condotte mediante il *malware* determinano una compressione al complesso di prerogative individuali inviolabili, dei quali gli artt. 14 e 15 Cost. rappresentano solo una porzione[194].

---

ivi, 1996, f. 12, p. 3268.

[192] Sul carattere di assolutezza della riserva di legge e di giurisdizione, da ultimo, Corte cost., 2 gennaio 2017, n. 20, in *Dir. pen. cont.*, 15 marzo 2017, con nota di E. ANDOLFATTO, *Il nuovo giudizio di legittimità costituzionale sulla sospensione del procedimento con messa alla prova: la consulta respinge tre questioni sollevate dal tribunale di Prato*. In dottrina, senza pretesa di completezza e limitandosi ad alcuni più recenti lavori, AA. VV., *Il diritto penale nella giurisprudenza costituzionale,* a cura di E. D'Orlando–l. Montanari, Giappichelli, 2009; M.A. CABIDDU–P. DAVIGO, *Leggi penali di favore ed efficacia* «in malam partem» *delle sentenze della Corte costituzionale*, in AA. VV., «*Effettività» e «seguito» delle tecniche decisorie della Corte costituzionale,* a cura di R. Bin–G. Brunelli–A. Pugiotto–P. Veronesi, Edizioni Scientifiche Italiane, 2006, p. 255 ss.; M. D'AMICO, *Corte costituzionale e discrezionalità del legislatore in materia penale*, in *Riv. AIC*, 17 novembre 2016, f. 4; ID., *Il principio di legalità in materia penale fra Corte costituzionale e Corti europee*, in AA. VV., *Le Corti dell'integrazione europea e la Corte costituzionale italiana*, a cura di N. Zanon, Edizioni Scientifiche Italiane, 2006, p. 167 ss.; A. LOLLO, *Norme penali di favore e zone d'ombra della giustizia costituzionale*, in *www.federalismi.it*, 29 giugno 2009, f. 13; I. PELLIZZONE, *Profili costituzionali della riserva di legge in materia penale. Problemi e prospettive*, Giuffrè, 2016; N. ZANON, *Corte costituzionale e norme penali di favore: verso un sindacato sulle scelte politico–criminali?*, in AA. VV., *Verso un sindacato di legittimità sulle scelte politico–criminali?,* a cura di L. Zilletti– F. Oliva, Edizioni ETS, 2007, p. 53 ss. Con precipuo riferimento al tema che qui rileva C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen., proc*., 2018, f. 9, p. 1213 ss.

[193] Per una puntuale disamina della libertà di corrispondenza così come tutelata dall'art. 8 CEDU, *ex multis*, M. BONETTI–A. GALLUCCIO, sub art. 8 *CEDU. Profili specifici*, in AA. VV., *Corte di Strasburgo e giustizia penale*, cura di G. Ubertis–F. Viganò, Giappichelli, 2016, p. 264 ss.; L. TOMASI, sub *art. 8,* in AA. VV., *Commentario breve alla Convenzione europea dei diritti dell'uomo,* a cura di S. Bartole–P. De Sena–V. Zagrebelsky, Cedam, 2012, p. 123 ss.; V. Zagrebelsky–R. Chenal–L. Tomasi, *Manuale dei diritti fondamentali in Europa*, Il Mulino, 2016, p. 23 ss.

[194] Sul tema, si rimanda a Cap. IV.

Più nel dettaglio, la possibilità di monitorare da remoto, segretamente e senza limiti spazio-temporali, ogni attività che il soggetto conduce, determina la proliferazione di minacce a diritti semi-nuovi, ossia prerogative tradizionali che assumono una differente fisionomia in ragione della necessità di offrire protezione alle esigenze dell'individuo informatizzato. Si pensi al rinnovato diritto alla riservatezza dei sistemi informatici[195], alla tutela del domicilio informatico[196], nonché al diritto all'intangibilità della vita digitale"[197], i quali rappresentano una proiezione nell'era moderna delle garanzie costituzionali coperte dalla doppia riserva, di legge e di giurisdizione. Di qui, mancando una previsione espresse per le funzioni del *malware* che esulano dall'attivazione del microfono per l'intercettazione tra presenti, sembra quasi che l'inquadramento delle tecniche di *remote forensics* nella categoria dei mezzi di ricerca della prova atipici sia funzionale ad aggirare le regole costituzionali, finendo per determinare «un'elusione delle garanzie»[198].

Su queste premesse, la dottrina si interroga sui limiti di utilizzo processuale delle risultanze investigative prodotte dall'impiego del *malware*.

Secondo alcuni Autori, poiché la legge interviene a disciplinare solo una delle possibili funzioni del *virus*, gli altri impieghi del *Trojan* dovrebbero essere ritenuti tendenzialmente inammissibili, anche ove tali meccanismi "assomiglino" a quelli propri di mezzi investigativi consentiti dal codice[199]: a fronte di interpretazioni più radicali che prospettano la necessità di ritenere le perquisizioni *on line* giuridicamente inesistenti perché carenti dei requisiti minimi indispensabili per integrare lo schema normativo dei mezzi investigativi[200], altra parte di dottrina rileva che le funzioni atipiche del captatore informatico, potenzialmente idonei a ledere beni giuridici protetti dalla riserva di legge e di giurisdizione, integrino un'ipotesi di prova incostituzionale[201] ovvero anticonvenzionale[202].

Dunque, secondo la ricostruzione offerta si prospetterebbero esiti procedimentali

---

[195] Diritto di matrice tedesca e "importato" in Italia dalla dottrina più avanguardista. In particolare, É la giurisprudenza costituzionale tedesca a consacrare espressamente il diritto all' "*Integrität und Vertraulichkeit informationstechnischer Systeme*". Cfr. BVerfG, 27 febbraio 2008, 370/2007-595/2007, in *BverfGE* 120, p. 274 ss. Per i riflessi sull'ordinamento nazionale, N. VENEGONI-L. GIORDANO, *La Corte costituzionale tedesca sulle misure di sorveglianza occulte e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Dir. pen. cont*., 8 maggio 2016.

[196] Il domicilio informatico «non è solo il luogo ove il soggetto avente diritto può esplicare liberamente qualsiasi attività lecita, ma è un'area la cui tutela si estende anche nello *ius excludendi alios* per cui si ritengono applicabili «tutte le garanzie previste al "domicilio tradizionale"». Cfr. Cass., sez. un., 7 febbraio 2012, n. 4694, in *www.neldiritto.it*. Nello stesso senso, sez. un., 24 aprile 2015, n. 17325, in *Proc. pen. giust*., 2015. Da ultimo, sez. V, 15 luglio 2019, n. 37339, in *C.E.D.* Cass., n. 277535; sez. II, 29 maggio 2019, n. 26604, *ivi*, n. 276427.

[197] Così denominato da S. SIGNORATO, *Le indagini digitali*, cit., p. 69.

[198] P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale,* cit., p. 342.

[199] P. BRONZO, *L'impiego del* trojan*,* cit., p. 346

[200] In questo senso M. DANIELE, Contrasto al terrorismo e captatori informatici, in *Riv. it. dir. proc. pen.,* 2017, f. 2, p. 402; L. PARLATO, *Problemi insoluti*, cit., p. 405

[201] Cfr. P. FELICIONI, *Le fattispecie "atipiche",* cit., p. 342; A. SANNA, *L'irriducibile atipicità,* cit., p. 611 ss.; M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.,* 2015, f. 9, p. 1168

[202] E. ANDOLINA, *L'ammissibilità degli strumenti di captazione dei dati personali tra standard di tutela della privacy e onde eversive*, in *Arch. pen*., 2015, f. 3, p. 9; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia*, p. 349.

diversi a seconda della tipologia di investigazione condotta dal *Trojan*. Qualora il captatore si limiti all'attivazione del microfono del dispositivo infettato, si integra un'ipotesi di intercettazione ambientale (e informatica) che trova regolamentazione espressa nella d.lgs. 216/2017; di qui il risultato ottenuto è utilizzabile nei limiti di cui agli artt. 266 ss. c.p.p. In relazione alla "altre" funzioni proprie del captatore informatico, deve ritenersi che i relativi risultati probatori non possano trovare impiego processuale, essendo affetti da incostituzionalità.

Non può, tuttavia, negarsi che la spiccata atipicità delle investigazioni esperibili mediate il *virus* non consente facilmente di distinguere nettamente le singole attività compiute, esponendo *de facto* lo strumento a possibili abusi legati al rischio che, a fronte dell'autorizzazione giurisdizionale all'immissione del *malware* per il compimento di una specifica attività – come quella di intercettazione ambientale – ne sia poi di fatto svolta un'altra, in sostituzione o in aggiunta, tendente, ad esempio a visualizzare i contenuti archiviati nella memoria del dispositivo[203].

Di conseguenza, sono le stesse caratteristiche della fattispecie e l'assenza di un adeguato modello legale di riferimento, a rendere disagevole il controllo da parte dell'autorità giudiziaria[204]. Di conseguenza, «[L]la verità è che il rischio di incidere su diritti fondamentali dell'individuo al di fuori dei confini tracciati dalla legge (costituzionale e ordinaria) è motivo sufficiente perché debbano ritenersi banditi dal processo penale gli strumenti investigativi le cui potenzialità intrusive non siano determinabili a priori»[205].

Segue il corollario: in un sistema governato dal canone di stretta legalità, deve ritenersi illegittimo qualsivoglia uso del captatore, in quanto, diversamente opinando, si determinerebbe una violazione degli artt. 14 e 15 Cost.[206].

Restano sul campo le esigenze investigative. L'irrinunciabilità di tali strumenti è evidente: pur comprimendo diritti fondamentali, i risultati ottenibili tramite il loro impiego sono assai efficaci nella persecuzione del crimine, per cui non è prospettabile che il processo ne rimanga privo.

Per tali ragioni, la dichiarazione di illegittimità per incostituzionalità delle perquisizioni *online*, con conseguente inutilizzabilità dei risultati acquisiti, non può rappresentare una conclusione, ma un punto di partenza: l'obiettivo non è quello di negare cittadinanza a tale strumento nel nostro ordinamento ma di stabilire a quali condizioni sia da considerarsi legittimo, tenuto conto dell'importanza che lo stesso va acquisendo ai fini di indagine e della crescente attenzione che a livello europeo e internazionale viene dedicata al tema.

È quindi compito del legislatore intervenire, dettando una disciplina *ad hoc*, che raggiunga un equo bilanciamento, alla luce del principio di proporzionalità, tra diritti

---

[203] La giurisprudenza di legittimità non sconfessa una simile impostazione. Come di recente chiarito, «[I]in tema di intercettazioni ambientali, la modifica delle modalità esecutive delle captazioni, concernendo un aspetto meramente tecnico, può essere autonomamente disposta dal pubblico ministero, non occorrendo un apposito provvedimento da parte del giudice per le indagini preliminari». Cass., sez. VI, 8 marzo 2018, n. 45468, in *Dir. pen. proc.,* 2019, f. 5, p. 697, con nota di C.R. BLEFARI, *Le intercettazioni nei confronti di soggetti non indagati.*

[204] In questo senso, A. CAMON, *Cavalli di Troia in Cassazione*, cit., p. 96.

[205] F. CAPRIOLI, *Il "captatore informatico",* cit., p. 501.

[206] Così A. SANNA, *L'irriducibile atipicità,* cit., p 617.

costituzionalmente protetti: quello alla riservatezza informatica da un lato e quello alla repressione dei reati dall'altro[207].

[207] In relazione a questo aspetto, è stato affermato che l'impiego del nuovo strumento esulerebbe dal raggio d'azione degli art. 14 e 15 Cost. e, dunque, non basterebbe l'introduzione di una specifica disciplina normativa, ma sarebbe necessario l'affermazione di un nuovo diritto fondamentale all'uso libero e riservato delle tecnologie informatiche, sul modello di quanto avvenuto in altri ordinamenti. R. ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen.* online, 25 luglio 2016. In particolare in Germania, a partire da una nota sentenza *Bundesverfassungsgericht*, 27 febbraio 2008, in *Riv. trim. dir. pen. econ*., 2009, f. 3, p. 679 e ss., con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del* Bundesverfassungsgericht *sulla c.d.* online durchsuchung., è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, ed è stato inaugurato un nuovo diritto costituzionale riconducibile alla c.d. "autodeterminazione informativa" e "sicurezza informatica", quest'ultima da intendersi anche come integrità e riservatezza dei dati e delle informazioni trattate da sistemi informatici, fondato sulla dignità umana dell'individuo e dell'utente "informatico". Nel 2016 è intervenuta un'altra pronuncia (*Bundersverfassungsgericht*, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09, in *Dir. pen. cont*., 8 maggio 2016, con nota di L. GIORDANO-A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici. Sull'esperienza europea in materia di perquisizioni* online, si rinvia a Cap. VI.

CAPITOLO III

LE APORIE APPLICATIVE DELLA NORMATIVA

SOMMARIO: 1. «Aspettando Godot»: la riforma dai "mille" rinvii. Uno sguardo d'insieme – 2. L'anomala limitazione degli apparecchi infettabili: il captatore informatico nei dispositivi elettronici "portatili" – 3. L'ossimoro ordinamentale: l'estensione dei reati intercettabili e la restrizione della nozione di criminalità organizzata – 4. I correttivi alla forza intrusiva del *virus*. Il decreto rafforzato – 4.1. *Segue*: l'insofferenza del *malware* alle predeterminazioni spazio-temporali – 5. Le irragionevoli limitazioni del potere del p.m. nella procedura d'urgenza – 6. Il nebuloso limite di operatività del *virus* nei delitti dei c.d. "colletti bianchi". Il tramonto del "doppio binario" – 6.1. *Segue*: questioni di diritto intertemporale. Il termine iniziale di efficacia delle nuove disposizioni – 7. Gli usi obliqui a fini investigativi. Il superamento dei limiti di inutilizzabilità procedimentale nella l. 7/2020 – 8. La fallace disciplina della conservazione del captato. La catena di custodia e la distruzione del *virus.*

1. «ASPETTANDO GODOT»*: LA RIFORMA DAI "MILLE" RINVII. UNO SGUARDO D'INSIEME

Come già detto più volte[1], la materia delle intercettazioni mediante captatore informatico rappresenta il frutto di una stratificazione legislativa e giurisprudenziale senza precedenti. Nonostante gli sforzi profusi, le nuove disposizioni, a distanza di oltre tre anni dal primo intervento riformatore, non trovano ancora compiuta realizzazione: questa vicenda, si è detto, «presenta i tratti del grottesco»[2].

Più nel dettaglio, la riforma operata dal d.lgs. 29 dicembre 2017, n. 216[3], in attuazione della delega contenuta nell'art. 1 della l. 23 giugno 2017, n. 103[4], sarebbe dovuta entrare in vigore il 26 luglio 2018 ma subisce nell'immediatezza tre rinvii con altrettanti provvedimenti normativi: la data del 31 marzo 2019 prevista dall'art. 2 del d.l. 25 luglio 2018, n. 91 viene prorogata al 31

*S. BECKETT, *Aspettando Godot*, 1952.

[1] Il complesso *iter* giurisprudenziale e normativo in materia di intercettazioni tramite captatore informatico è stato oggetto di trattazione autonoma nel Cap. I.

[2] L'espressione appartiene a M. GIALUZ, *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare*, in *Sist. pen.,* 1 maggio 2020. Nello stesso senso, G. SANTALUCIA, *Delitti dei c.d. colletti bianchi e intercettazioni tra presenti su dispositivo portatile: termine iniziale di efficacie delle nuove disposizioni. Spunti dalla sentenza n. 741 delle Sezioni unite civili,* in *Sist, pen.,* 2020, n. 4, p. 5 ss. Come precisato da L. FILIPPI, *Intercettazioni:* habemus legem!, in *Dir. pen. proc*., 2020, f. 4, p. 453, «[L]la lunga gestazione della riforma […] si è poi conclusa, tra le doglie, con un aborto spontaneo». Secondo F. RUGGIERI, *La nuova disciplina delle intercettazioni: alla ricerca di una lettura sistematica*, in *Proc. pen. giust.,* 2020, f. 4, p. ?, «[S]se a questa circostanza si aggiunge che anche la recente legge 28 febbraio 2020 n. 7 di conversione del d.l. 30 dicembre 2019 n. 161 ha a sua volta novellato e modificato l'articolato del codice di rito relativo a tale mezzo di ricerca della prova contenuto nel provvedimento d'urgenza, *prima facie* non sembra possibile offrire una visione sistematica e soprattutto coerente dell'istituto».

[3] Cfr. d.lgs. 29 dicembre 2017, n. 216, recante "*Disposizioni in materia di intercettazioni di conversazioni o comunicazioni, in attuazione della delega di cui all'articolo 1, commi 82, 83 e 84, lettere a), b), c), d) ed e), della legge 23 giugno 2017, n. 103*", in *Gazz. uff.,* 11 gennaio 2018, n. 8.

[4] L. 23 giugno 2017, n. 103, recante "*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*", in *Gazz. uff.,* 4 luglio 2017, n. 154.

luglio 2019[5] e successivamente rinviata al 31 dicembre 2019[6]. Poi, proprio nel giorno della sua entrata in vigore, il Consiglio dei Ministri, con una manovra alquanto repentina, approva la contro-riforma del sistema intercettazioni[7]. Il che, sebbene inaspettato perché improvviso, non sorprende. La divergenza di vedute tra l'*ex* Ministro della Giustizia, Andrea Orlando, e quello attuale, Alfonso Bonafede, era nota ai più: tra il mese di giugno e luglio 2018, subito dopo il varo del primo Governo di Giuseppe Conte, il Ministro aveva già espresso pubblicamente l'intento di avviare una "riforma della riforma" in tempi brevi quale correttivo al contuso sistema giustizia[8].

Secondo la novella del 2019, la normativa avrebbe dovuto trovare applicazione ai procedimenti penali iscritti dopo il 29 febbraio 2020. Naturalmente, si è trattato di un termine irrealistico, «tanto da far sorgere il dubbio che fosse stato inserito solo per asseverare l'urgenza dell'intervento e giustificare il ricorso alla decretazione d'urgenza»[9].

Puntualmente, in sede di conversione, il Parlamento prospetta tempi ragionevolmente più lunghi, facendo slittare l'entrata in vigore tra il 30 aprile e il 1 maggio[10]. Ma ulteriori rinvii non tardano ad arrivare. Subito dopo l'approvazione della legge 7/2020, il mondo intero si accinge a combattere la lotta pandemica contro il Covid-19; la nuova emergenza da contenere impedisce evidentemente di completare quelle «complesse misure organizzative in atto, anche relativamente alla predisposizione di apparati elettronici e digitali» e di effettuare «le attività di collaudo dei sistemi presso i singoli uffici giudiziari delle procure della Repubblica» in modo da «giungere all'entrata in vigore della disciplina con le misure organizzative completamente dispiegate e funzionanti»[11]. Così il 30 aprile 2020, viene procrastinata nuovamente l'entrata in vigore della normativa, stabilendo che le nuove disposizione si applicheranno nell'ambito dei procedimenti penali iscritti dopo il 31 agosto 2020[12].

---

[5] *Ex* art. 1, comma 1139, lett. *a* della l. 30 dicembre 2018, n. 145, recante "*Bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021*", in *Gazz. uff*., 31 dicembre 2018, n. 302.

[6] Secondo il disposto dell'art. 9, comma 2, d.l. 14 giugno 2019, n. 53, recante "*Disposizioni urgenti in materia di ordine e sicurezza pubblica*", convertito, con modificazioni, dalla l. 8 agosto 2019, n. 77, in *Gazz. uff*., 9 agosto 2019, n. 186.

[7] D.l., 30 dicembre 2019, n. 161, recante "*Disposizioni urgenti in materia di intercettazioni*", in *Gazz. uff*., 31 dicembre 2019, n. 305, convertito, con modificazioni, dalla l. 28 febbraio 2020, n. 7, in *Gazz. uff*., 28 febbraio 2020, n. 50.

[8] Il 22 giugno 2018, intervenendo a un convegno organizzato dal Consiglio Superiore della Magistratura, il Ministro della Giustizia Bonafede aveva dichiarato: «il mio impegno prioritario è capire le linee della riscrittura del provvedimento e su questo avvierò un confronto già la prossima settimana con procure e avvocati». F. CACCIA, *Bonafede all'Anm: intercettazioni, bloccherò la riforma*, in *Corriere della Sera*, 2018, 23 giugno 2018, p. 11.

[9] M. GIALUZ, *L'emergenza nell'emergenza: il decreto-legge n. 28 del 2020, tra ennesima proroga delle intercettazioni, norme manifesto e "terzo tempo" parlamentare,* cit.

[10] Sul punto G. SPANGHER, *La riforma sconta due mesi di proroga, in vigore dal 1° maggio*, in *Guida dir.*, 2020, n. 13, p. 34.

[11] Con queste motivazioni era stato giustificato lo slittamento dell'entrata in vigore alla fine di febbraio: v. *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019*, reperibile al sito *www.senato.it*., p. 7. V. al riguardo G. AMATO, *Un differimento per ragioni tecniche e organizzative*, in *Guida dir.,* 2020, n. 6, p. 65.

[12] D.l. 30 aprile 2020, n. 28, recante "*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*", in *Gazz. uff*., 30 aprile 2020, n. 111. CONVERSIONE.

Da una lettura organica della normativa si evince la volontà del legislatore (sia del 2017 che del 2019) di recepire gli orientamenti giurisprudenziali[13] e le istanze dottrinali[14] che animano, ormai da qualche tempo, il dibattito politico, giuridico e sociale. Non sempre, però, i suggerimenti degli "addetti ai lavori" hanno trovato terreno fertile nelle riforme e il risultato finisce per nascondere molte insidie per la tenuta del sistema e l'efficacia stessa dello strumento intercettivo[15].

I dubbi e le perplessità non derivano soltanto dal discutibile contenuto della normativa – e, dunque, dalle scelte di politica legislativa di cui si parlerà tra breve – ma anche dagli orientamenti di politica criminale sottesi alle riforme.

In relazione a questo secondo aspetto, si evidenzia che lo stravolgimento della disciplina in materia di intercettazioni interviene con modalità alquanto anomale, ricorrendo al duttile strumento del decreto legge[16].

---

[13] Cfr. Cass., sez. VI, 26 maggio 2015, n. 27100, in *Dir. giust*., 29 giugno 2015; sez. un., 28 aprile 2016, n. 26889, in *Arch. pen*., 2016, n. 2, p. 348 ss.; sez. VI, 3 maggio 2016, n. 27404, in *Quot. Giur*., 2016; sez. VI, 3 maggio 2016, n. 26054, non massimata; sez. VI, 3 maggio 2016, n. 26058, non massimata; sez. VI, 13 giugno 2017, n. 36874, in *Dir. pen. cont.*, 27 settembre 2017; sez. VI, 28 febbraio 2017, n. 15573, in *C.E.D. Cass*., n. 269950; sez. V, 20 ottobre 2017, n. 48370, in *Giur. it.,* 2017, n. 11, p. 2498; sez. I, 28 giugno 2017, n. 29169, in *Cass. pen*., 2018, f. 4, p. 343 ss.; sez. VI, 8 marzo 2018, n. 45468, in *Dir. pen. proc.*, 2019, f. 5, p. 697. Da ultimo, sez. I, 25 giugno 2019, n. 50972, in *C.E.D. Cass*., n. 277862. Sul punto anche diverse pronunce di merito. Cfr. Tribunale di Modena, 28 settembre 2016, in *www.giurisprudenzapenale.com*; Tribunale di Milano, 13 maggio 2016, in *www.dejure.it*; Tribunale di Palermo, sez. riesame, 11 gennaio 2016, in *www.penalecontemporaneo.it*; Tribunale di Roma, sez. I, 10 agosto 2015, in *www.dejure*.it.

[14] Compendiata nell'istanza dei numerosi docenti di diritto che reclamano l'introduzione di una disciplina *ad hoc*. Cfr. AA.VV., *Necessaria una disciplina legislativa in materia di captatori informatici (c.d.* "trojan"): *un appello al legislatore da parte di numerosi docenti di diritto italiani*, in *Dir. pen. cont.*, 7 ottobre 2016.

[15] Sulle criticità del complesso normativo, L. FILIPPI, *D.l. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, in *Il quotidiano giuridico*, 10 gennaio 2020; M. GRIFFO, *Il* Trojan *e le derive del terzo binario. Dalla riforma Orlando al d.l. 161/2019, passando per la "spazzacorrotti" e il decreto sicurezza* bis, in *Sist. pen*., 2020, f. 2, p. 61 ss.; ID., *Rilievi sull'impiego del* trojan *nei procedimenti per i reati contro la pubblica amministrazione*, in *Proc. pen. giust*., 2020, n. 2, p. 482 ss.; W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, *ivi,* 2020, f. 1, p. 63 ss.; C. PARODI, *Convertito il d.l. 161/2019 in materia di intercettazioni: le correzioni di rotta,* in *www.ilPenalista.it,* 26 febbraio 2020; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, *ivi*, 2020, f. 1, p. 109 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni, ivi,* 2020, f. 2, p. 71 ss.; *La metamorfosi delle intercettazioni, ultimo atto? La legge n. 7/2020 di conversione del d.l. 161/2019*, in *www.sistemapenale.it,* 2 marzo 2020; G. SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni, ivi*, 2020, f. 1, p. 47 ss.: A. SCALFATI, *Intercettazioni: spirito autoritario, propaganda e norme inutili*, in *Arch. pen*., 2020, f. 1, p. 1; G. SPANGHER, *Dl intercettazioni: una controriforma dall'avvio incerto*, in *Guida dir.,* 2020, n. 10, p. 14; ID., *La riforma sconta due mesi di proroga, in vigore dal 1° maggio*, *ivi*, 2020, n. 13, p. 34.

[16] Evidenziando tali perplessità L. FILIPPI, *D.l. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, cit.; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità,* cit., p. 112; W. NOCERINO, *Prime riflessioni*, cit., p. 64. Sulle discutibili scelte di politica legislativa e criminale, anche G.M. FLICK, *Intercettazioni. Intervista*, su *Il Dubbio*, 29 febbraio 2020, pubblicata su *Cass. pen.,* 2020, f. 5, p. 1804 ss. Più in generale, sull'inopportunità di affidare al d.l. la normazione "ordinaria", M. BENVENUTI, *Alle origini del decreto legge. Saggio sulla decretazione governativa d'urgenza e sulla genealogia dell'ordinamento giuridico dell'Italia*

A ben guardare, soprattutto nell'ultimo tempo, si assiste a riforme e controriforme finalizzate a placare l'inquietudine dell'elettorato attivo; profonde modifiche che stravolgono il sistema penale e processuale realizzate con leggi delega e "rappezzate" con suggestivi, imprevedibili e talvolta inopportuni decreti legge che fungono da correttivi alla normativa previgente[17].

Per quel che in questa sede rileva, si nota come il legislatore, nell'attuare i criteri direttivi della legge delega del 2017, innovi la disciplina in chiave securitaria, ampliando prepotentemente l'ambito operativo del *virus* informatico che, da strumento "eccezionale" da impiegare solo allorquando i medesimi risultati investigativi non possano essere raggiunti ricorrendo agli strumenti tradizionali di indagine, diventa regola cui ricorrere nell'ottica di una semplificazione e velocizzazione dei tempi delle indagini. La medesima *voluntas legis* permea le novelle successive che, utilizzando un metodo "inversamente proporzionale", ne estendono l'applicazione abbattendo i limiti agli impieghi obliqui dei risultati appresi[18].

Sul versante delle scelte di politica criminale, il provvedimento sembra il collettore di istanze e pulsioni caratterizzate da *input* molto diversi tra loro, che il legislatore non riesce però a

---

prefascista, in Studi in onore di Claudio Rossano, Jovene, 2013, p. 21 ss.; A. CELOTTO, *L'abuso del decreto–legge. Volume I: Profili teorici, evoluzione storica e analisi morfologica*, Cedam, 1997, *passim*; D. CHINNI, *La decretazione d'urgenza tra abusi e controlli. Qualche considerazione quindici anni dopo la sentenza n. 360 del 1996 della Corte costituzionale*, in *Dir. e soc*., 2012, f. 1, p. 55; E. DI AGOSTA, *Democrazia, legalità, politica criminale dell'emergenza. L'uso del decreto legge in materia penale,* in *Cass. pen*., 2014, f. 9, p. 3149 ss.; L. ELIA, *Sui possibili rimedi all'abuso della decretazione d'urgenza*, in AA. VV., *Decreti–legge non convertiti*, Atti del seminario svoltosi in Roma, Palazzo della Consulta, 11 novembre 1994, Giuffrè, 1996, p. 187 ss.; F. FONDERICO, *Una riscrittura delle norme piegata all'emergenza che mette in un angolo la certezza del diritto*, in *Guida dir*., 2013, f. 37, p. 55; E. MARZADURI, *Il ricorso alla decretazione d'urgenza condizionato dal diffuso allarme sociale*, in *Guida dir*., 2009, f. 10, p. 39 ss.; R. ROMBOLI, *Decreto legge e giurisprudenza della corte costituzionale*, in AA. VV., *L'emergenza infinita. La decretazione d'urgenza in Italia,* a cura di A. Simoncini, EUM, 2006, p. 19 ss. Da ultimo, S. LORUSSO, *Il cigno nero nel processo penale*, in *Sist. pen.,* 11 maggio 2020, per il quale «[…] una volta tanto, la necessità e l'urgenza erano reali e non una mera clausola di stile apposta nella premessa di un decreto-legge per giustificarne l'emanazione bypassando il confronto in Parlamento […]». Come evidenziato in altre occasioni, secondo l'Autore «la cultura dell'emergenza è divenuta un dato strutturale della legislazione italiana in materia di giustizia penale, sempre caratterizzata da interventi disarticolati e disomogenei, frutto di decretazione d'urgenza o di iniziative parlamentari e governative avviate senza la dovuta ponderazione, a seguito del clamore suscitato da qualche fatto di cronaca». Così S. LORUSSO, *Il fascino discreto dell'emergenza*, in AA. VV., *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Cedam, 2008, p. XXI. Sul tema, già G. GROTTARELLI DÈ SANTI, *Uso e abuso del decreto–legge,* in *Dir. e società*, 1978, p. 241 ss., e G. RICCIO, *Politica penale dell'emergenza e Costituzione,* Edizioni Scientifiche italiane, 1982, p. 59 ss., il quale s'interroga sulla legittimità di un monopolio governativo, gestito attraverso la decretazione d'urgenza, in tema di politica penale, «[N]nel senso che ci si domanda se esso, condizionato da "casi straordinari di necessità ed urgenza", rispetti e rispecchi i principi fondamentali di un moderno diritto penale».

[17] In questo senso L. FILIPPI, *D.l. intercettazioni: abrogata la riforma Orlando, si torna all'antico*, cit. Come, tuttavia, evidenziato, «l'occasione e la ragione per il legislatore di intervenire con lo strumento della decretazione d'urgenza sono state la straordinaria necessità e urgenza di perfezionare e completare la nuova disciplina delle intercettazioni telefoniche e ambientali prima che la stessa acquisiti efficacia […], nonché la straordinaria necessità e urgenza che le modifiche apportate rientrino in vigore prima che sia applicabile la disciplina dettata dal d.lgs. n. 216/2017 e che tale termine sia coordinato con le esigenze di adeguamento degli uffici requirenti dal punto di vista strutturale e organizzativo». Così *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019,* cit., p. 1.

[18] Ci si riferisce alla L. 9 gennaio 2019 n. 3, recante «*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*», in *Gazz. uff.,* 16 gennaio 2019, n. 13 e alla l. 28 febbraio 2020, n. 7, cit.

comporre. Il dato emerge dalla mancanza di organicità dell'impianto strutturale; dagli innesti poco coordinanti con l'assetto vigente, dalle scelte stilistiche alquanto ridondanti, contraddittorie e, talvolta, non perfettamente pertinenti al contesto di riferimento, tanto da confondere l'interprete.

Inoltre, il legislatore attuale – assai più cauto di quello del 2017 – opera un "*restyling* conservativo" della materia senza rinunciare a spunti di modernità[19]: pochi i cambiamenti radicali ma molteplici i ritocchi sintattici e semantici alle disposizioni originarie, operati attraverso interventi di microchirurgia normativa, in modo da sperimentare un sistema che, almeno da un punto di vista concettuale, si presenti agile e moderno.

Al di là di posizioni più o meno critiche nei confronti della disciplina gradualmente costruita, l'interprete può ritenersi soddisfatto di alcune innovative riflessioni di metodo.

In primo luogo, non può non apprezzare l'attenzione posta dal legislatore ad un tema "caldo" come quello delle intercettazioni a mezzo di captatore informatico: consapevole dei rischi connessi all'utilizzo dell'inedito strumento di indagine, ritiene di dover procedere all'adozione di una disciplina che si propone di offrire una regolamentazione – tutt'altro che esaustiva, stante la "fretta" degli interventi riformatori – della nuova tecnica intercettiva.

In particolare, l'introduzione di una specifica disciplina in materia di captatore informatico risponde al bisogno, oramai non più procrastinabile, di adeguare l'obsoleto codice di rito al progresso scientifico-tecnologico degli ultimi anni. A ben guardare, infatti, il ricorso ad evoluti sistemi di supervisione e controllo da remoto non solo crea frizione in relazione ai tradizionali precetti riconosciuti nella Carta fondamentale [20], ma comporta anche la proliferazione di minacce a diritti di "terza generazione", propri di una "società 2.0", atti a tutelare le nuove esigenze di un individuo informatizzato e impongono un salto qualitativo nell'individuazione di norme volte a garantirlo[21]. Di qui, può sostenersi che la «disciplina vigente nasce […] da una ponderazione degli interessi in gioco che va ricalcolata» [22].

Un dato, tuttavia, appare ineludibile. La nuova disciplina in materia di captazioni tramite *virus* informatico sembra scontrarsi con la *ratio* ispiratrice della riforma in tema di intercettazioni: se da una parte, il legislatore impone un rigoroso rispetto del diritto alla *privacy*, nell'ottica del principio di proporzione e adeguatezza, dall'altra, estendendo la portata del rinnovato istituto senza prevedere inibizioni alle altre attività di controllo che il captatore è in grado di eseguire, non sembra efficacemente garantito il diritto alla riservatezza personale e digitale, contribuendo a delineare un sistema investigativo improntato al controllo e al monitoraggio degli individui – anche indirettamente – coinvolti.

---

[19] Come meglio si specificherà di seguito, la novella non modifica in maniera sostanziale la disciplina introdotta nel 2017 che, nella sostanza, rimane pressochè inviariata, se non in relazione all'uso extraprocedimentale dei dati acquisiti.

[20] Quali l'art. 13 Cost., baluardo della libertà di ogni individuo, l'art. 14 Cost., posto a protezione del domicilio, l'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, nonché il principio di proporzionalità che impone, ai sensi dell'art. 8 CEDU, la necessità di una perfetta corrispondenza tra i risultati perseguiti e i mezzi adoperati e, più in particolare, tra la potenziale forza invasiva del mezzo in esame e l'inevitabile lesione dei diritti fondamentali. Inoltre le attività captative creano punti di frizione con il rinvigorito diritto alla riservatezza e la *privacy* soprattutto in relazione al "nuovo pacchetto protezione dei dati UE" che ne rafforza la tutela attraverso un processo di armonizzazione comunitaria. Cfr. Regolamento europeo 2016/679 (GDPR, *General Data Protection Regulation*), relativo alla *Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, entrato in vigore il 24 maggio 2016.

[21] Su cui si rinvia a Cap. IV.

[22] P. BRONZO, *Intercettazione ambientale,* in AA. VV., *Nuove norme in tema di intercettazione,* cit., p. 236.

Il *vulnus* arrecato ai diritti fondamentali è ancora più intollerabile allorquando la normativa di riferimento non risulti sufficientemente chiara e dettagliata circa i casi e i modi che legittimano una siffatta compressione. Più precisamente, la legislazione compulsiva intervenuta in materia determina un sistema multiforme, un complesso disciplinare magmatico dai confini alquanto incerti, sbiaditi e, molto spesso, solo tratteggiati, facendo sorgere dubbi interpretativi che lasciano agli operatori del diritto ampi margini di manovra, contribuendo a rafforzare quella prassi deviata per cui è la giurisprudenza a dominare la legge, la consuetudine a trionfare nel processo. E il risultato che ne deriva è quello di una riforma alquanto sbilanciata in favore delle esigenze investigative di cui è portatrice la Magistratura: in questo senso depone tutto quel complesso di modifiche che tende ad adeguare il diritto vigente a quello vivente, a lenire le conflittualità legalizzando prassi deviate che, spesso, nel segno della prevalenza della sostanza rispetto alla forma, attentano i diritti fondamentali dei protagonisti del processo.

Si assiste ad una ulteriore manifestazione del fenomeno per cui è il legislatore a recepire consuetudini e costumi processuali anzicchè il contrario: diventano legge giurisprudenza, prassi, *soft law.* Così il "grigiore" del quadro normativo consente il ricorso alle più svariate e astruse sfumature, atte a riempire gli spazi vuoti che il legislatore – dolosamente o per negligenza – non intende colorare: «il fronte sistemico esprime l'innegabile debolezza della legalità, non la colloca più sul versante del dominio della legge […], avendo assunto essa […] il significato di premessa ordinante la disciplina del processo comunque affidate, per il diritto, all'interpretazione giudiziarie e, per la loro realizzazione, alle prassi operanti nella giurisdizione»[23].

Dunque, sono questi i paradigmi da considerare per cogliere le matrici delle distorsioni prasseologiche che segnano l'epopea del captatore informatico nel processo penale, evidentemente da correggere al fine di ripristinare un sistema democratico di giustizia in cui la legalità diventa metodo e non fine.

2. L'ANOMALA LIMITAZIONE DEGLI APPARECCHI INFETTABILI: IL CAPTATORE INFORMATICO NEI DISPOSITIVI ELETTRONICI "PORTATILI"

Nell'ottica di contenere l'area di interesse del *virus*, in nome delle garanzie fondamentali potenzialmente "attentate" dallo smodato impiego dello strumento in fase investigativa, il legislatore prevede che la peculiare modalità captativa possa avvenire esclusivamente inoculando il *malware* su un dispositivo elettronico *target* dotato del carattere della "portabilità"[24].

In sostanza, le nuove regole si riferiscono soltanto alla possibilità di "infettare" dispositivi mobili, lasciando privo di tipizzazione e di regolamentazione il possibile impiego del captatore

[23] Si esprime così M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, Editoriale Scientifica, 2019, p. 17.

[24] *Ex* art. 266, comma 2, primo periodo, c.p.p. «[L]l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita […]». L'emendamento n. 36.4000 al Disegno di legge n. 2067 A.S., intitolato "*Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole di processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*", approvato dal Senato il 15 marzo 2017, prevedeva di disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in «dispositivi informatici e telematici», anziché in «dispositivi elettronici portatili». Cfr. F. RUGGIERI, *L'impatto delle nuove tecnologie informatiche: il captatore informatico L'art. 1 c. 84 lett. e del d.d.l. Orlando: attuazione e considerazioni di sistema*, in *Jus*, 28 ottobre 2017, p. 355.

informatico su apparecchiature fisse, come PC connessi ad internet, *smart-tv*, telecamere di sicurezza dotate di microfono[25].

Nella sua ermeticità, la norma presta il fianco a plurime interpretazioni.

Secondo un'esegesi più rigorosa del dettato normativo, si potrebbe ritenere che il silenzio normativo stia a significare che l'inoculazione in dispositivi fissi non possa essere consentita neppure in presenza dei presupposti che giustificano l'intercettazione di comunicazioni tra presenti[26].

Viceversa, accogliendo un'interpretazione più flessibile del *dictum*, si potrebbe ipotizzare che l'omesso riferimento all'inoculazione su dispositivi fissi derivi dalla convinzione del legislatore per cui spia fisica e spia elettronica rappresenterebbero due tecniche assolutamente fungibili; conseguentemente, l'installazione da remoto della cimice elettronica risulterebbe senz'altro consentita dalle norme generali in tema di intercettazione ambientale[27].

Differenti ragioni inducono l'interprete ad optare per quest'ultima soluzione.

Intanto, è proprio la *littera legis* del disposto codicistico a suggerire tale opzione. Invero, l'art. 266, comma 2 c.p.p. consente l'intercettazione itinerante «anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile». Ed è proprio la congiunzione "anche" a far propendere l'interprete per un'esegesi "allargata" del dettato normativo, quasi come se il legislatore avesse voluto rappresentare ed esplicitare il riconoscimento di un'intercettazione i cui contorni spaziali non sono definibili a priori; *nulla quaestio*, invece, nel caso di captazioni statiche, dal momento che il *virus* informatico, perdendo la sua intrinseca itineranza, svolgerebbe la medesima funzione della tradizionale microspia[28].

In secondo luogo, sono ragioni di coerenza sistemica a sorreggere la scelta *de qua*: se è possibile installare una microspia in un determinato luogo, al fine di captare tutte le comunicazioni che avvengono all'interno del "raggio di portata" della cimice, sarebbe irragionevole ipotizzare che al medesimo risultato non si possa giungere tramite la più agevole inoculazione del *virus* informatico in un dispositivo elettronico fisso, stante la facile indicazione nel decreto autorizzativo del luogo in cui si trova l'apparecchio da sottoporre a monitoraggio.

Inoltre, la limitazione degli apparati infettabili risulterebbe contraddittoria rispetto alla normativa introdotta per regolamentare l'impiego del *virus Trojan* nei reati corruttivi: a ben guardare, infatti, gli innesti normativi operati dalla l. 3/2019 e dalla l. 7/2020 dimostrano come il

---

[25] Sottolinea l'incongruenza di una simile disposizione, S. ATERNO, *Il punto di vista degli operatori. Il difensore*, in AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra-R. Orlandi, Giappichelli, 2018, p. 331. Si evidenzia, a tal proposito, la proposta dell'Avv. Stefano Aterno presentata presso la Commissione giustizia del Senato il 4 febbraio 2020, per cui sarebbe opportuna l'eliminazione della preclusione in esame in ragione delle attività – che ormai da diversi anni (Cfr. Cass., sez. V, 14 ottobre 2009, n. 16556, in *C.E.D. Cass.,* n. 246954) – si conducono con il captatore informatico anche sui computer fissi. Cfr. S. Aterno, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, *www.senato.it,* p. 3.

[26] In questo senso P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* in. *Riv. it. sc. giur*., 2017, f. 8, p. 345.

[27] Accoglie una simile impostazione O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, in *Dir. pen. cont*., 2018, f. 11, p. 69 s.

[28] In questo senso D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont*., 2018, f. 1, p. 217, secondo cui «nessun problema si pone nel caso di infezione di un dispositivo non portatile posto che l'attivazione del microfono garantisce comunque la sicura determinabilità del luogo in cui avvengono le captazioni. Diversa è la questione nel caso di apparati che, in ragione della loro portabilità, consentono intercettazioni ubiquitarie».

legislatore abbia inteso legittimare senza inibizioni l'uso del captatore informatico in relazione ai delitti commessi ai danni della pubblica amministrazione. Di qui, l'esclusione dell'operatività del *malware* dagli apparati fissi – di cui normalmente sono dotati gli uffici pubblici – sembra stridere con la *ratio* che sottende l'intervento riformatore[29].

D'altra parte, il divieto di inoculare il *virus* sui dispositivi fissi avrebbe un certo "costo", non pienamente giustificato in termini di efficienza investigativa: come precisato, «esso renderebbe inevitabile – ove l'intercettazione ambientale sia indispensabile ai fini della prosecuzione delle indagini – l'impiego delle tecnologie "tradizionali", e dunque il posizionamento all'interno del luogo oggetto di indagine di un una cimice "fisica", il che può comportare un certo rischio per gli operanti, e può presentare un più alto margine di fallimento rispetto alla metodica del *malware* informatico»[30].

Di qui, pur nella consapevolezza del rischio di legittimare un utilizzo "libero" dei *malware*, l'impiego del *virus* deve ritenersi consentito sia per infettare apparati fissi che mobili: al fine di evitare illogicità sistemiche, sembra possibile fornire un'interpretazione adeguatrice del rinnovato apparato codicistico e ammettere le intercettazioni virali (non itineranti) anche se effettuate ai danni di un dispositivo fisso installato (anche) in un luogo di privata dimora, a condizione che, in questo ultimo caso, vi sia il fondato motivo di ritenere che *ivi* si stia svolgendo un'attività criminosa o che si proceda per uno dei gravi delitti di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p, ovvero per quelli commessi dai pubblici ufficiali o dagli incaricati di pubblico servizio.

3. L'OSSIMORO ORDINAMENTALE: L'ESTENSIONE DEI REATI INTERCETTABILI E LA RESTRIZIONE DELLA NOZIONE DI CRIMINALITÀ ORGANIZZATA

L'elemento nucleare della riforma è rappresentato dalla delimitazione dell'ambito di operatività dello strumento investigativo, con specifico riguardo alle fattispecie di reato intercettabili mediante l'impiego del captatore informatico.

La novella introduce un «doppio binario di disciplina»[31], tracciando una netta distinzione tra i delitti di criminalità mafiosa e assimilati e tutte le altre tipologie di reato per cui sono ammesse le intercettazioni. In particolare, ai sensi del comma 2 *bis* dell'art. 266 c.p.p., l'intercettazione ambientale mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile «è sempre consentita» nei procedimenti per i delitti di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p., nonché – per effetto dell'intervento riformatore del 2019, poi avallato ed ampliato dal legislatore nel 2020 – nei procedimenti gravi di criminalità economica commessi dai pubblici ufficiali e dagli incaricati di pubblico servizio[32]; viceversa, per tutti gli altri delitti è ammessa nel

[29] Cfr. W. NOCERINO, *Prime riflessioni a margine del nuovo decreto legge in materia di intercettazioni*, cit.

[30] Rileva una simile criticità P. BRONZO, *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 345.

[31] Così A. BALSAMO, *Il punto di vista degli operatori. Il magistrato*, in AA. VV., *Nuove norme in tema di intercettazione*, cit., p. 344.

[32] Si precisa che nel corso della presente trattazione si terrà in considerazione solo la scelta legislativa relativa all'impiego disinibito del *Trojan* nei reati distrettuali; mentre non si farà cenno alle altre fattispecie delittuose ricomprese nel regime derogatorio di cui all'art. 266, comma 2 *bis* c.p.p., dal momento che l'esegesi della normativa che ha ad oggetto le intercettazioni mediante captatore informatico per i procedimenti relativi ai reati commessi dai pubblici ufficiali e dagli incaricati di pubblico servizio ai danni della pubblica amministrazione, sarà oggetto di specifico approfondimento. Cfr. §?

domicilio «solo se vi è fondato motivo di ritenere che *ivi* si stia svolgendo l'attività criminosa», così come previsto dal comma 2 del medesimo articolo.

Nel delineare il perimetro operativo della nuova forma di intercettazione, il legislatore sembra assai confuso e poco coerente con le logiche del sistema, dal momento che le possibilità di impiego del *Trojan* risultano, al contempo, lievemente ridotte e notevolmente estese: per un verso, infatti, viene fornita un'interpretazione "restrittiva" del concetto di criminalità organizzata, ricomprendendovi solo le fattispecie indicate nell'art. 51 commi 3 *bis* e 3 *quater* c.p.p., escludendo, invece, quelle facenti capo ad un'associazione per delinquere, *ex* art. 416 c.p.; per l'altro, viene ampliata la portata del *virus*, consentendo di utilizzare il captatore per tutti i reati per cui sono ammissibili le intercettazioni ambientali, nel rispetto dei requisiti di cui all'art. 266 c.p.p.

Con riferimento al primo aspetto, non può sottacersi come il legislatore, nell'accogliere una nozione assai parca di "criminalità organizzata", operi una scelta alquanto coraggiosa che disattende gli orientamenti giurisprudenziali oramai consolidati sul punto[33]. Mancando nel sistema nazionale qualsivoglia definizione di criminalità organizzata[34], la prassi tende ad

[33] Come noto, la categoria di "criminalità organizzata" viene sempre più spesso intesa come un *genus* aperto, per nulla coincidente con quello dei reati di stampo mafioso o aggravati dall'art. 7, l. 203 del 1991. In giurisprudenza, cfr., Cass., sez. un., 22 marzo 2005, n. 17706, in *Cass. pen*., 2005, f. 10, p. 2916 ss., con nota di G. MELILLO, *Appunti in tema di sospensione feriale dei termini relativi a procedimenti per reati di criminalità organizzata*, per cui la nozione di criminalità organizzata «identifica non solo i reati di criminalità mafiosa e assimilata, oltre i delitti associativi previsti da norme incriminatrici speciali, ma anche qualsiasi tipo di associazione per delinquere, *ex* art. 416 c.p., correlata alle attività criminose più diverse, con l'esclusione del mero concorso di persone nel reato, nel quale manca il requisito dell'organizzazione». Nello stesso senso sez. III, 18 luglio 2015, n. 36927, in *C.E.D. Cass*., n. 265023; sez. II, 25 novembre 2015, n. 6321, *ivi*, n. 266404. Con specifico riguardo al tema del captatore informatico, Cass., sez. un., 28 aprile 2016, n. 26889, cit.; sez. VI, 3 maggio 2016, n. 26054, cit.; sez. maggio 2016, n. 26055, cit.; sez. VI, 3 maggio 2016, n. 26058, non massimata; sez. VI, 13 giugno 2017, n. 36874, cit., con nota di L. GIORDANO, *La prima applicazione della sentenza "Scurato" nella giurisprudenza di legittimità*, per cui «[l]in considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso». Per un'accurata disamina dell'evoluzione dottrinale e giurisprudenziale, v. M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 50 ss.

[34] A differenza di tutti gli altri ordinamenti di *civil law* ovvero di *common* law, il sistema italiano conosce cinque varianti di criminalità organizzata: a) la criminalità organizzata comune, ovvero quella riconducibile allo schema dell'associazione per delinquere prevista dall'art. 416 c.p., che si riscontra in tutti i casi nei quali un gruppo di persone si associa per la realizzazione di delitti comuni; b) l'associazione di tipo mafioso, disciplinata dall'art. 416 *bis* c.p., che si concretizza quando il sodalizio pone in essere delitti o addirittura attività lecite (quali il controllo di attività economiche, l'acquisizione di concessioni o appalti, il condizionamento di voti favorevoli durante le competizioni elettorali) attraverso un metodo mafioso, caratterizzato dalla intimidazione e dalla omertà che ne deriva; c) le associazioni c.d. monotematiche, ovvero quelle costituite esclusivamente per la gestione di singole attività delittuose (associazione contrabbandiera, art. 291 *quater* del Testo Unico Leggi Doganali, per il commercio dei tabacchi lavorati esteri, associazione per il traffico di stupefacenti, art. 74 del Testo Unico Stupefacenti, associazione finalizzata alla tratta degli essere umani, art. 416 c.p. sesto comma, ecc.); d) le associazioni con finalità di terrorismo o di eversione dell'ordine democratico, *ex* artt. 270 ss. c.p.

avallarne una nozione così tanto ampia da valorizzare le specifiche finalità della disciplina che deroga le regole processuali generali[35] (c.d. approccio teleologico o finalistico)[36].

Pertanto, in detta categoria vengono ricomprese attività criminose alquanto eterogenee, purché realizzate da una pluralità di soggetti i quali, per la commissione del reato, abbiano costituito un apposito apparato organizzativo, con esclusione del mero concorso di persone *ex* art. 110 c.p.; ad essa non sono riconducibili solo i reati di criminalità mafiosa ma tutte le fattispecie criminose di tipo associativo. In altri termini, «basta la costruzione di un apparato organizzativo la cui struttura organizzativa assuma un ruolo preminente rispetto ai singoli partecipi»[37].

L'*overrulling* legislativo, funzionale a limitare la nozione di criminalità organizzata ai soli reati "distrettuali", mostra una certa sensibilità verso i parametri introdotti di determinatezza e prevedibilità che devono caratterizzare l'atto intercettivo secondo la giurisprudenza europea[38].

---

[35] *Ex* art. 13, d.l. 13 maggio 1991, n. 152, recante "*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*", in *Gazz. uff.,* 13 maggio 1991, n. 110, convertito, con modificazioni, in l. 12 luglio 1991, n. 203, in *Gazz, uff.*, 12 luglio 1991, n. 162. Per i reati di criminalità organizzata e terrorismo, la norma prevede dei requisiti "attenuati" rispetto a quelli tradizionali: le intercettazioni tra presenti possono essere condotte anche nel domicilio a prescindere dal «fondato motivo di ritenere che in quel luogo si stia consumando un'attività criminosa»; l'intercettazione è ammessa sulla basi di «sufficienti indizi» (e non gravi, *ex* art. 267 c.p.p.), quando la stessa è «necessaria» (e non indispensabile *ex* art. 267 c.p.p.) alla prosecuzione delle indagini; la durata delle operazione non può superare i 40 giorni, prorogabili di 20. Di qui, per i reati "gravi" non contemplati dagli artt. 51, commi 3 *bis* e 3 *quater*, richiamati dall'art. 266, comma 2 *bis* c.p.p., sono ammesse le intercettazioni ambientali domiciliari senza alcun limite se si tratta di captazioni "tradizionali"; viceversa, se le stesse sono eseguite mediate captatore, soggiacciono al requisito di cui al comma 2 dell'art. 266. Inoltre, è per questi previsto l'obbligo di motivazione "rafforzata" con l'indicazione dei tempi e dei luoghi della captazione, secondo il disposto dell'art. 267, comma 1 c.p.p. Sul tema, per tutti, D. MANZIONE, *Una normativa "d'emergenza" per la lotta alla criminalità organizzata e la trasparenza e il buon andamento dell'attività amministrativa (d.l. 152/1991 e l. n. 203/1991): uno sguardo d'insieme*, in *Legislaz. pen*., 1992, p. 852 ss. La normativa viene progressivamente ampliata, ai sensi dell'art. 3 del d.l. 18 ottobre 2001, n. 374, recante "*Disposizioni urgenti per contrastare il terrorismo internazionale*" ai procedimenti per i delitti di cui all'art. 270 *ter* c.p.p. e ai delitti delineati dall'art. 407, comma 1, lett. *a*, n. 4 c.p.p., nonché ai delitti di cui agli artt. 270, comma 3 e 306, comma 2 c.p.p. Inoltre, l'art. 9 l. 11 agosto 2003, n. 228 estende l'applicazione delle disposizioni di cui all'art. 13 d.l. 13 maggio 1991, n. 152, in relazione ai procedimenti per i delitti previsti dal Libro II, Titolo XII, Capo III, Sez. I c.p. (al netto delle ipotesi ricomprese nell'art. 51, comma 3 *bis*, c.p.p.), nonché a quelli previsti dall'art. 3, l. 20 febbraio 1958, n. 75. Sul punto, più di recente, L. SIMEONE, *I reati associativi,* Maggioli editore, 2015, p. 53 ss.

[36] In questa prospettiva, le Sezioni Unite "Scurato" hanno ribadito la validità dell'approccio "teleologico" o "finalistico" secondo il quale il significato dell'espressione "criminalità organizzata" deve essere definito avendo riguardo alle finalità specifiche della singola disciplina che deroga alle regole processuali generali. La sentenza ha ritenuto di dover confermare la validità di questo indirizzo giurisprudenziale, «perché consente di cogliere l'essenza del delitto di criminalità organizzata e nel contempo di ricomprendere tutti i suoi molteplici aspetti, nell'ottica riconducibile alla ratio che ha ispirato gli interventi del legislatore in materia, tesi a contrastare nel modo più efficace quei reati che per la struttura organizzativa che presuppongono e per le finalità perseguite, costituiscono fenomeni di elevata pericolosità sociale». Così Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[37] Si esprime così P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 247.

[38] Corte EDU, 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 66610/10, in *www.archiviopenale.it*. In tema, E. BASILICO-S. MARIANI, *Monitoraggio Corte Edu dicembre 2015*, a cura di G. Ubertis- F. Viganò, in *Dir. pen. cont.,* 15 marzo 2016.

Più nel dettaglio, la sentenza della Corte EDU "Zakharov c. Russia", nel delineare un nuovo «statuto europeo delle intercettazioni»[39], ribadisce che le legislazioni nazionali devono definire l'ambito applicativo delle misure di controllo dando ai cittadini un'adeguata indicazione delle circostanze per cui le autorità pubbliche hanno il potere di ricorrervi, anche mediante una chiara definizione della natura dei reati che possono dare luogo al loro impiego. Pur non richiedendo un elenco puntuale, la Corte europea ritiene che debbano essere forniti sufficienti dettagli sulla natura di tali reati, ad esempio mediante la indicazione del massimo di pena edittale per essi prevista; «difficile allora ritenere soddisfatto questo *standard* nella nostra nozione giurisprudenziale»[40]. In questo senso, è apparso ineludibile ricorrere ad un criterio più preciso – come quello dei reati "distrettuali" che trovano una regolamentazione espressa nell'art. 51 c.p.p. – e dunque fatalmente più restrittivo, proprio al fine di garantire il pieno rispetto dei *dicta* europei.

Al di là di queste ipotesi, però, le possibilità di impiego del nuovo strumento risultano enormemente ampliate.

In ragione del richiamo compiuto dall'*incipit* del comma 2 dell'art. 266 c.p.p. al comma 1 del medesimo articolo, l'inoculazione del *virus* informatico diventa possibile in qualsiasi tipologia di indagine, purchè si tratti di reati per i quali le intercettazioni tradizionali sono ritenute legittime[41].

Tale disposto va letto anche alla luce dell'innesto legislativo operato nel 2020, per cui il catalogo di fattispecie intercettabili si dilata nuovamente. Più precisamente, la l. 7/2020 procede

---

[39] Così A. BALSAMO, *Le nuove frontiere delle intercettazioni telefoniche*, in *Il Libro dell'anno del diritto*, Treccani, 2017, p. 4.

[40] Così P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 245 s. Cfr. tuttavia A. BALSAMO, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen*., 2016, f. 12, p. 4236, il quale – senza però esprimersi in ordine al modo in cui la giurisprudenza interpreta la clausola generale della "criminalità organizzata" – nota come una tale nozione, per quanto contrassegnata da un certo grado di elasticità, «non sembra di per sé incompatibile con i requisiti qualitativi insiti nel principio di legalità nella prospettiva europea, che non esclude formulazioni normative idonee ad assicurare un costante adeguamento al mutare della materia regolata».

[41] Nelle intercettazioni tradizionali il catalogo di reati per cui l'attività investigativa risulta legittima sembra assai ampio e variegato, potendosi esperire captazioni processuali per tutte le fattispecie di cui all'art. 266, comma 1 c.p.p. ovvero, nel caso di intercettazioni di comunicazioni informatiche o telematiche di cui all'art. 266 *bis* c.p.p., anche per i reati commessi mediante l'impiego di tecnologie informatiche o telematiche. In particolare, il legislatore individua i reati per cui sono consentite le intercettazioni prevalentemente sulla base di un criterio di natura quantitativa, incentrato sull'entità della pena edittale, determinata a norma dell'art. 4 c.p.p. Si tratta dei delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni, ovvero per i delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni. In altri casi, il legislatore utilizza un criterio qualitativo, indicando i reati–tipo per cui è esperibile il mezzo di ricerca della prova (delitti concernenti sostanze stupefacenti o psicotrope; quelli concernenti le armi e le sostanze esplosive; delitti di contrabbando; reati di ingiuria, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, molestie; divulgazione di materiale pedopornografico e adescamento di minorenni; *stalking.* Da ultimo, la l. 7/2020 estende i casi di intercettazione anche ai «delitti commessi avvalendosi delle condizioni previste dall'art. 416 *bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste nello stesso articolo»). Sul tema, esaustivamente, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 479 ss.; A. CAMON, *Le intercettazioni nel processo penale*, cit., p. 64; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale*, Giappichelli, 2016, p. 172 ss.; L. FILIPPI, sub *art. 266,* cit., p. 2571 s.; G. ILLUMINATI, *La disciplina processuale delle intercettazioni,* cit., p. 74 s.; S. FURFARO, voce *Intercettazioni (profili di riforma),* cit., già pubblicato in *Arch. pen*., f. 1, 2018; E. MARZADURI, *Spunti per una riflessione sui presupposti applicativi delle intercettazioni telefoniche a fini probatori*, in *Cass. pen*., 2008, f. 11, p. 4833 ss.

ad una modifica dell'art. 266, comma 1 c.p.p. attraverso l'interpolazione di un'inedita lettera "f-*quinquies*", introducendo una nuova *species* di reato intercettabile anche mediante l'ausilio del *virus* informatico, rappresentata dai «delitti commessi avvalendosi delle condizioni previste dall'art. 416 *bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste nello stesso articolo»[42].

Si tratta di una scelta alquanto avventata.

Come meglio si dirà di seguito[43], la possibilità di inoculare un *malware* su un dispositivo elettronico portatile in uso all'indagato per qualsivoglia tipologia delittuosa, determina – almeno in potenza – la violazione del *dictum* di cui all'art. 266, comma 2 c.p.p., posto a protezione del domicilio (art. 614 c.p.)[44]: in ragione dell'intrinseca itineranza dello strumento *de quo*, non

---

[42] Come rilevato, «[L]la norma […] si riferisce ai "delitti-fine" di un'associazione mafiosa, di per sé già suscettibile di giustificare un provvedimento di autorizzazione. Può ritenersi discutibile che in tal modo qualsiasi delitto, anche di relativamente di minor gravità (se la relativa pena superasse il limite edittale di cui all'art. 266 c.p.p. le intercettazioni sarebbero già ammissibili), possa giustificare il ricorso al mezzo di ricerca della prova in esame, sol perché motivato dai caratteri propri di un'associazione di stampo mafioso». Così F. RUGGIERI, *La nuova disciplina delle intercettazioni: alla ricerca di una lettura sistematica*, cit., p. ?

[43] Cfr. § ?

[44] In base all'evoluzione giurisprudenziale, può dirsi che i luoghi "domiciliari" sono quei luoghi in cui il titolare possiede uno *ius excludendi alios* stabile, ovvero azionabile anche quando il soggetto non sia fisicamente presente. Come precisato, il carattere di "stabilità" del diritto risulta, ai fini della determinazione del concetto di domicilio, assolutamente necessario. Rientrano, pertanto, nella nozione di domicilio solo i luoghi che assolvono in concreto alla finalità di proteggere la vita privata del loro possessore, durante lo svolgimento delle sue attività professionali, di svago, di alimentazione, di riposo. In questo senso, G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione*, in AA. VV., *Le nuove intercettazioni*, cit., p. 139 s. Detto in altri termini, affinché scatti la protezione prevista da tale articolo, non basta che un comportamento venga tenuto in un luogo di privata dimora, in quanto occorre che esso sia in concreto riservato, e, cioè non possa in concreto essere liberamente osservato dagli estranei, senza ricorrere a particolari accorgimenti. Cfr. Corte cost., 7 maggio 2008, n. 149, in *Cass. pen*., 2008, f. 12, p. 4109. Seguendo un simile filone interpretativo, può sostenersi che è considerato domicilio un ufficio privato (Cass., sez. VI, 29 settembre 2003, n. 4933, in *Cass. pen*., 2005, f. 10, p. 1336), mentre non sono tali le stanze di un ospedale (sez. V, 11 ottobre 2018, n. 5300, in *C.E.D. Cass.,* n. 27592) o le celle carcerari (sez. VI, 15 maggio 2018, n. 26028, *ivi*, n. 273417), il pianerottolo di un'abitazione privata (sez. 5, 30 maggio 2017, n. 34151, *ivi,* n. 270679), il *box* cassa di un'autorimessa (sez. V, 17 novembre 2015, n. 11419, in *Cass. pen*., 2017, f. 2, p. 722 ss., con nota di C. RIZZO, *Videoregistrazioni domiciliari e l'incerta distinzione tra comportamenti comunicativi e non)*. Sul punto, V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa,* in *Proc. pen. giust*., 2019, f. 2, p. 336 ss. In proposito la giurisprudenza della Suprema corte ha, ormai, disposto che l'autovettura non può essere considerata un luogo di "privata dimora", in quanto quest'ultima è destinata al trasporto «di persone o al trasferimento di oggetti da un luogo ad un altro ed in quanto sfornito dei confort minimi per potervi risiedere stabilmente per un apprezzabile lasso di tempo [...]» Così sez. I, 6 maggio 2008, n. 32851, in *Cass. pen*., 2009, f. 8, p. 2533. Da ultimo, sez. VI, 30 gennaio 2019, n. 23819, in *C.E.D. Cass.,* n. 275994. La delicata *quaestio* sembra aver trovato una stabilità ermeneutica grazie al recente apporto delle sezioni unite che accoglie un'interpretazione maggiormente restrittiva alla nozione *de qua*. Cfr. Cass., sez. un., 23 marzo 2017, n. 31345, in *Dir. pen. cont*., 2017, f. 7/8, con nota di S. BERARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624* bis *c.p.,* secondo cui «rientrano nella nozione di privata dimora di cui all'art. 624 *bis* c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare». Per una ricostruzione storica della nozione di privata dimora v. L. FILIPPI, sub *art. 226*, in *Codice di procedura penale commentato*, cit., p. 2541 ss.

risultano preventivabili i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto; di conseguenza, non può essere verificato il rispetto della condizione di legittimità richiesta dalla norma che presuppone, per la legalità delle captazioni in luoghi domiciliari nel caso di reati "comuni", che sia in atto l'attività criminosa[45].

Come noto, il giudice autorizza l'intercettazione nei luoghi di privata dimora solo quando, attraverso un giudizio *ex ante*, ritenga verosimilmente e ragionevolmente sussistente il *periculum* che in quel luogo si stia consumando un'attività delittuosa[46]: a meno che il progresso tecnologico non consentisse di predeterminare il funzionamento del *virus*, circoscrivendo il luogo in cui la captazione debba avvenire, l'agente intrusore è «fisiologicamente incompatibile con la necessità di dimostrare […] il fondato motivo di ritenere che in un determinato luogo si stia svolgendo un'attività criminosa»[47].

Proprio per la possibile lesione alla libertà domiciliare, la giurisprudenza pregressa è stata alquanto rigorosa sul punto, negando l'utilizzo dello strumento intercettivo nel caso di procedimenti per reati comuni, consentendolo solo per i reati di criminalità organizzata per cui la prerogativa di cui all'art. 266, comma 2 c.p.p., viene meno per effetto della disciplina derogatoria di cui all'art. 13, d.l. 152/1991[48].

Di qui, al fine di evitare indebite compressioni al *dictum* di cui all'art. 266, comma 2 c.p.p., sarebbe stato più opportuno limitare l'impiego del captatore informatico per eseguire intercettazioni (o, più correttamente, attività di acquisizione da remoto) solo con precipuo riguardo ai reati distrettuali di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., al fine di garantire il pieno rispetto della garanzia di tutela dei luoghi domiciliari.

Né può condividersi l'approccio di una parte della dottrina[49] che tenta di superare le difficoltà or ora richiamate ricorrendo ad una nozione estensiva di "domicilio", idonea a ricomprendere proprio il dispositivo infettato.

---

[45] Per i reati "diversi", tuttavia, la Suprema Corte esclude l'utilizzo dello strumento intercettivo, in quanto, non potendo prevedere i luoghi di privata dimora in cui il dispositivo infettato potrebbe essere introdotto – in qualità di captazioni "itineranti" –, non sarebbe possibile verificare il rispetto del *dictum* di cui all'art. 266 comma 2 c.p.p. Cass., sez. un., 28 aprile 2016, n. 26889, cit. Sul punto, si rinvia a Cap. I, § ?.

[46] Cfr. Cass., sez. I, 12 dicembre 1994, n. 1367, in *C.E.D. Cass.*, n. 200242.

[47] Si esprime così M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Giuffrè, 2017, p. 39.

[48] Cass., sez. un., 28 aprile 2016, n. 26889, cit.; sez. VI, 3 maggio 2016, n. 26054, cit.; sez. maggio 2016, n. 26055, cit.; sez. VI, 3 maggio 2016, n. 26058, non massimata; sez. VI, 13 giugno 2017, n. 36874, cit. Va, tuttavia, segnalato che, già prima dell'intervento riformatore del 2017, la giurisprudenza ha tentato di estendere il perimetro applicativo del *virus*, prevedendo che «ai fini dell'utilizzabilità delle intercettazioni di comunicazioni tra presenti mediante l'installazione di un "captatore informatico", consentite nei soli procedimenti di criminalità organizzata, è ammissibile, da parte del tribunale del riesame, la riqualificazione come reato appartenente a tale categoria del fatto esposto nella richiesta di autorizzazione del pubblico ministero e nel provvedimento emesso dal G.i.p., in quanto ciò che conta è che il fatto, sebbene sussunto sotto altre figure di reato, sia qualificabile come delitto di criminalità organizzata». Così Cass., sez. VI, 28 febbraio 2017, n. 15573, in *C.E.D. Cass.*, n. 269950. Per un esame di questa sentenza, v. L. GIORDANO, *Intercettazioni per mezzo di captatore informatico: il tribunale può riqualificare il fatto esposto nel decreto del Gip*, in *Ilpenalista.it*, 15 dicembre 2017. Nello stesso senso sez. I, 28 giugno 2017, n. 29169, in *Cass. pen.*, 2018, f. 4, p. 343 ss., con nota di L. GIORDANO, *Le prime applicazioni della sentenza "Scurato" nella giurisprudenza di legittimità*. Ma già sez. VI, 21 luglio 2015, n. 34809, in *C.E.D. Cass.*, n. 264447; sez. VI, 22 novembre 2007, n. 47109, *ivi*, n. 238715.

[49] In questo senso S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 244.

Secondo una simile impostazione, il luogo di privata dimora nel quale viene effettuata l'intercettazione itinerante non si rinverrebbe nello spazio fisico nel quale è presente il dispositivo elettronico portatile infettato, bensì nello *smartphone* stesso. In altre parole, il captatore rappresenterebbe la cimice, mentre il domicilio sarebbe configurato dall'apparato su cui il *malware* viene inoculato, a condizione che quest'ultimo soddisfi «i requisiti dello *ius includendi se*; dello *ius includendi et excludendi alios* e della destinazione del luogo ad attività private tipiche della vita domestica o a spazio di attività lavorativa»[50]. Come corollario di tale lettura, il fondato motivo di ritenere che si stia svolgendo l'attività criminosa dovrebbe essere riferito al dispositivo elettronico portatile infetto, e non al luogo fisico in cui avviene l'intercettazione, rimanendo così del tutto residuale l'ipotesi di intercettazione itinerante al di fuori di un luogo di cui all'art. 614 c.p.

Pur rappresentando una soluzione al *vulnus* che l'itineranza intrinseca del captatore arreca al domicilio, l'opzione ermeneutica *de qua* non sembra trovare conferme nel dettato normativo "ritoccato": se il legislatore avesse voluto configurare il dispositivo elettronico quale luogo di privata dimora, avrebbe provveduto ad adeguare la procedura autorizzativa alla nuova *species* di intercettazione nel domicilio informatico; per converso, l'art. 267 c.p.p. richiama (e rafforza) i presupposti legittimanti le intercettazioni nel caso in cui la captazione avviene mediante *Trojan*[51], richiedendo la precisazione dei (tempi e dei) luoghi in cui l'impiego del *virus* può dirsi legittimo e per i quali i relativi risultati investigativi non solo colpiti da inutilizzabilità[52].

4. I CORRETTIVI ALLA FORZA INTRUSIVA DEL *VIRUS*. IL DECRETO RAFFORZATO

Con il precipuo intento di attribuire al *virus* il carattere di "eccezionalità", il legislatore sceglie di regolamentare minuziosamente la forma e il contenuto del decreto autorizzativo: quasi come un palliativo al male inferto dalle infinite e indefinite potenzialità investigative del captatore informatico, si introducono regole assai stringenti a cui l'autorità giudiziaria deve soggiacere per legittimare il compimento delle operazioni intercettive.

In primis, attraverso un'interpolazione del comma 1 dell'art. 267 c.p.p., il decreto con cui l'autorità giudiziaria acconsente alle intercettazioni mediante *Trojan* assumere le vesti di un

---

[50] Cfr. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 246.

[51] Se si seguisse la suddetta lettura sarebbe necessario domandarsi quale valore semantico attribuire alla nozione di indicazione di luoghi "indirettamente determinati" di cui all'art. 267, comma 1 c.p.p. *Prima facie* potrebbe sostenersi che i luoghi sarebbero sempre determinati, poiché non si comprende come il dispositivo bersaglio possa essere indicato indirettamente. Tuttavia, il dispositivo bersaglio in uso a un soggetto determinato potrebbe non essere sempre il medesimo: l'utenza (*rectius*: lo *smartphone*) oggetto di intercettazione potrebbe essere ceduta dal proprietario a un terzo; ovvero potrebbe accadere che il dispositivo *target* presenti dei malfunzionamenti o diventi inutilizzabile per i più vari motivi e, quindi, venga sostituito l'organismo ospite. L'indicazione dei luoghi in modo indiretto, quindi, potrebbe riassumersi in formule generiche del tipo «il dispositivo mobile appartenente a Tizio», non specificando la marca e il numero seriale dello stesso, così consentendo l'intercettazione itinerante anche nel caso di successione nel tempo di dispositivi mobili. In questo senso O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 63. Si tratta, tuttavia, di un'interpretazione alquanto forzata, non trovandosi riscontri in alcuna norma riformata. Sul punto, v. § 4.1.

[52] Ai sensi dell'art. 271, comma 1 c.p.p., per cui «[I]i risultati delle intercettazioni non possono essere utilizzati qualora le stesse siano state eseguite fuori dei casi consentiti dalla legge o qualora non siano state osservate le disposizioni previste dagli articoli 267 e 268 commi 1 e 3».

provvedimento corredato da una motivazione "rafforzata", dovendo indicare le specifiche ragioni che rendono necessaria la peculiare modalità operativa[53].

I nuovi criteri direttivi impongono, quindi, al giudice «uno sforzo giustificativo ulteriore»[54]: non solo quello di indicare nel decreto autorizzativo le ragioni per cui l'intercettazione risulta «assolutamente necessaria alla prosecuzione delle indagini»[55] – ossia «l'obbligo di spiegare il perché di un'intercettazione»[56] – e la sussistenza dei «gravi indizi di reato»[57], ma anche il motivo

---

[53] Sul contenuto del decreto autorizzativo, si consenta un rinvio a D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in AA. VV., *Le recenti riforme in materia penale*, a cura di G.M. Baccari-C. Bonzano-K. La Regina- E.M. Mancuso, Wolters Kluwer-Cedam, 2017, p. 560. Sul punto v. P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 249; ID., *L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 342 ss.; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Rev. Bras. de Direito Processual Penal,* Porto Alegre, 2017, vol. 3, f. 2, p. 497 s.; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 219.

[54] Così P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 249.

[55] Ai sensi dell'art. 267 c.p.p., il p.m. richiede al g.i.p. l'autorizzazione a disporre le operazioni d'intercettazioni qualora ritenga sussistenti gravi indizi di reato, da valutare nel rispetto dei criteri di cui all'art. 203 c.p.p., e che l'attività sia assolutamente indispensabile ai fini della prosecuzione delle indagini. In relazione a quest'ultimo requisito, il g.i.p. è tenuto a verificare che dell'impiego di tale strumento investigativo non si possa fare a meno in ragione della particolare natura della fattispecie criminosa per cui si procede, ovvero della speciale piega che lo sviluppo delle intercettazioni dovesse aver preso. Sul tema la dottrina è assai vasta. Limitandoci ai lavori di carattere più generale, E. APRILE, *Intercettazioni di comunicazioni,* in AA. VV., *Trattato di procedura penale,* t. 1, v. 2, a cura di A. Scalfati, diretto da G. Spangher, Utet, 2009, p. 475 ss.; E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuovi questioni giuridiche*, Giuffrè, 2004, p. 108 ss.; P. BALDUCCI, *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria,* Giuffrè, 2002; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. disc. pen*., VII, Utet, 2001, p. 175 ss.; A. BARGI, voce *Intercettazioni di comunicazioni e conversazioni*, *ivi,* III, 2005, p. 790 ss.; A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale,* Giappichelli, 2016, p. 199 ss.; G. CONSO, *Intercettazioni telefoniche: troppe e troppo facilmente divulgabili*, in *Dir. pen. proc.,* 1996, f. 1, p. 137 ss.; M.L. DI BITONTO, *Lungo la strada per la riforma della disciplina delle intercettazioni,* in *Cass. pen*., 2008, f. 1, p. 18 ss.; L. FILIPPI, sub *art. 267*, in *Codice di procedura penale commentato*, a cura di A. Giarda–G. Spangher, V ed., Wolters Kluwer, 2017, p. 2622 ss.; ID., *Intercettazione,* in AA. VV., *La prova penale,* a cura di P. Ferrua–E. Marzadura– G. Spangher, Giappichelli, 2013, p. 837; ID., *L'intercettazione di comunicazioni*, Giuffrè, 1997; G. GIOSTRA, *Intercettazioni tra indagini e* privacy, in *Dir. e giust*., 2006, f. 31, p. 98 s.; V. GREVI, *Le intercettazioni come mero "mezzo di ricerca" di riscontri probatori?*, in *Cass. pen*., 2009, f. 6, p. 848 ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007; D. SIRACUSANO–F. SIRACUSANO, *Le prove*, in AA. VV., *Diritto processuale penale*, a cura di G. Di Chiara–V. Patanè–F. Siracusano, Giuffrè, 2018, p. 318 s.; C. PARODI, *Le intercettazioni. Profili operativi giurisprudenziali*, Giappichelli, 2002, p. 88 ss.; G. SPANGHER, *Linee guida per una riforma delle intercettazioni telefoniche*, in *Dir. pen. proc*., 2008, f. 9, p. 1209 s. In chiave critica, più di recente, F. ALONZI, *La Costituzione impone rigore nell'interpretare i presupposti applicativi delle intercettazioni telefoniche*, in *Arch. pen.* online, 2016, p. 1.

[56] Si esprime così, V. GREVI, *L'obbligo di spiegare il "perché" di un'intercettazione,* in *Corriere della sera*, 14 aprile 2014.

[57] Come precisato dalla dottrina, «[È]è evidente come tale formula sia ben diversa da quella dei "gravi indizi di colpevolezza", di cui all'art. 273, comma 1 c.p.p. […] e, infatti, in materia di intercettazione è necessario verificare la sussistenza di elementi di prova gravi, tali cioè da potere, sulla base degli stessi, affermare, con un giudizio di qualificata probabilità, che esiste uno dei reati per i quali è possibile autorizzare l'impiego di tale mezzo di prova, senza effettuare alcun controllo circa la

per cui si ritiene «necessaria» la peculiare forma di captazione. E ciò tanto per l'autorizzazione a procedere per i reati "comuni" che per quelli "distrettuali". Come, infatti, precisato, «il regime dell'art. 13 d.l. n. 152 del 1991 – e oggi quello delle intercettazioni ambientali tramite *Trojan* per i reati distrettuali – esonera il giudice dallo specificare i motivi per cui ritiene che nei luoghi *ex* art. 614 c.p. si stia svolgendo l'attività criminosa, ma non lo esime dall'argomentare in ordine alla necessità […] di disporre quella intercettazione per acquisire elementi alle indagini»[58].

Una scelta, questa, funzionale – almeno in astratto – a limitare l'impiego del *malware* ai soli casi nei quali si riscontrano specifiche esigenze investigative che giustificano il ricorso allo strumento *de quo,* nel pieno rispetto del principio di proporzione in sede di applicazione dell'istituto.

A ben guardare, però, la "necessità" prevista non equivale al requisito dell'"indispensabilità" che, per converso, non è richiesta dal dato normativo. Sulla base di un simile distinguo, si evince che non è necessaria la prova del fatto che il ricorso a tale peculiare forma di intercettazione sia l'unico strumento operativo praticabile, dal momento che «il giudizio di necessità non coincide con quello di certa infruttuosità delle altre forme di intercettazione ambientale quanto piuttosto con la prova […] di una meno agevole praticabilità delle operazioni tradizionali»[59].

A parere di chi scrive, sarebbe stata preferibile una maggiore attenzione da parte del legislatore nella precisazione dei parametri che il provvedimento autorizzativo avrebbe dovuto detenere per giustificare il ricorso al captatore informatico, al fine di contenere il rischio di interpretazioni distorte del dettato normativo, evitando, al contempo, un probabile lassismo dell'autorità giudiziaria in sede operativa.

In effetti, se si seguissero gli orientamenti giurisprudenziali più recenti in tema di intercettazioni "tradizionali", il provvedimento autorizzativo «deve [solo] contenere una adeguata e specifica motivazione a concreta dimostrazione del corretto uso del potere dal giudice esercitato»[60], ritenendo di poter escludere l'utilizzabilità del decreto solo qualora «la motivazione sia apparente, semplicemente ripetitiva della formula normativa, del tutto insufficiente e inadeguata rispetto al provvedimento che dovrebbe giustificare»[61]. In questi casi, il rischio potrebbe essere quello del ricorso a mere formule di stile, attraverso le quali si assicura il rispetto di quel *quantum* di motivazione richiesto per l'idoneità del decreto che deve consistere in quello

---

riferibilità soggettiva di quel reato a un determinato soggetto». Così E. APRILE, *Intercettazioni di comunicazioni,* cit., p. 483. Sul punto, v. anche M. BORGOBELLO, *La motivazione degli atti di autorizzazione e relativi vizi,* Giappichelli, 2013, p. 55 ss. Nello stesso senso la giurisprudenza di legittimità. Cfr. Cass., sez. II, 20 febbraio 2003, n. 11023, in *C.E.D. Cass*., n. 223913. Inoltre, si è detto che «[…] il presupposto dei gravi indizi di reato va inteso non in senso probatorio, ossia come valutazione del fondamento dell'accusa, ma come vaglio di particolare serietà delle ipotesi delittuose configurate, le quali non devono risultare meramente ipotetiche, essendo al contrario richiesta una sommaria ricognizione degli elementi dai quali sia dato desumere la seria probabilità dell'avvenuta consumazione di un reato». Così sez. VI, 26 febbraio 2010, 10902, in *C.E.D. Cass.,* n. 246688. Nello stesso senso, sez. V, 17 novembre 2016, 1407, *ivi*, n.268900; sez. III, 2 dicembre 2014, n. 14954, *ivi*, n. 263044.

[58] Così P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 254.

[59] In questi termini D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 219.

[60] Cfr. Corte cost., 4 aprile 1973, n. 34, in *Giur. cost*., 1973, p. 326 ss.

[61] Così Cass., sez. un., 21 giugno 2000, n. 17, in *Cass. pen*., 2001, f. 1, 69 ss. Nello steso senso anche la giurisprudenza successiva. Più di recente, sez. I, 18 febbraio 2019, n. 11168, in *C.E.D. Cass*., n. 274996; sez. II, 29 maggio 2018, n. 55199, *ivi*, n. 274252; sez. VI, 4 novembre 2014, n. 53420, *ivi* n. 261839.

«minimo necessario a chiarire le ragioni del provvedimento»[62], senza addentarsi nella precisazione delle ragioni che impongono l'uso del *virus*.

Proprio al fine di scongiurare simili *pericula*, le intercettazioni di conversazioni o comunicazioni tra presenti tramite agenti intrusori avrebbero dovuto rappresentare l'ultimo gradino della scala gerarchica dei mezzi di ricerca della prova esperibili, l'*extrema ratio* cui ricorrere solo quando tutti gli altri strumenti cognitivi – tra cui le tradizionali intercettazioni – non sarebbero stati in grado di soddisfare le esigenze investigative del caso concreto, con riguardo all'alto rischio di infruttosità delle operazioni intercettive condotte tramite gli strumenti tradizionali.

D'altra parte, una maggiore rigorosità normativa in relazione alla precisazione delle ragioni investigative che impongono il ricorso al captatore informatico sarebbe stata necessaria non solo per assicurare la piena realizzazione della funzione di garanzia che il decreto autorizzativo dovrebbe svolgere contro eventuali abusi[63] ma anche per disincentivare le procure all'assidua richiesta dello strumento in esame, temendo che – nel caso di istanza basata su presupposti effimeri e, dunque, un conseguente provvedimento giudiziario carente nel precisare la necessarietà delle operazioni *de qua* – il decreto autorizzativo possa essere affetto da invalidità per difetto di motivazione.

4.1. *SEGUE*: L'INSOFFERENZA DEL *MALWARE* ALLE PREDETERMINAZIONI SPAZIO-TEMPORALI

La peculiarità del decreto autorizzativo nel caso di intercettazione mediante captatore informatico non si esaurisce nell'introduzione del presupposto della "necessarietà" investigativa quale condizione legittimante il ricorso allo strumento in esame: al fine di porre rimedio alla spiccata intrusività del *virus* nella sfera della riservatezza, infatti, il legislatore introduce ulteriori requisiti che aggravano ulteriormente l'onere motivazionale del giudicante.

Più in particolare, ai sensi dell'art. 267, comma 1 c.p.p., il provvedimento con cui si autorizzano le operazioni di intercettazione tramite captatore informatico deve indicare «i luoghi e il tempo, anche se indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono»[64].

---

[62] Cass., sez. V, 27 maggio 2004, n. 5001, in *Guida dir*., 2004, f. 26, p. 76 ss.

[63] L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* in *Dir. pen. cont.*, 2017, f. 3, p. 177 ss. Conformemente, A. TESTAGUZZA, voce Virus *informatico*, in *Dig. disc. pen*., X, Utet, 2018, p. 931 ss.; ID., *I sistemi di controllo remoto: fra normativa e prassi,* in *Dir. pen. proc*., 2014, f. 6, p. 764, per cui «[I]in questa prospettiva va letta l'esigenza di far recuperare al decreto autorizzativo una funzione di garanzia ai fini di un migliore bilanciamento tra diritti costituzionali confliggenti, attraverso una motivazione che dia conto dell'indispensabilità del mezzo probatorio richiesto ai fini della prosecuzione delle indagini rispetto ad una determinata e seria ipotesi delittuosa, rifuggendo da espressioni apodittiche e meramente ripropositive del contenuto delle norme». C'è, poi, chi, mostrando una maggiore sensibilità al tema, auspica che il soggetto legittimato a "disporre" le intercettazioni sia proprio lo stesso giudice che le abbia autorizzate. Tale conclusione, favorirebbe un controllo costante sui diritti del singolo, sottraendolo ad una delle parti del processo, «non fosse altro che per il rispetto di elementari esigenze di equilibrio in relazione a diritti individuali più facilmente vulnerabili da chi, istituzionalmente, è preposto ad altro». Così A. GAITO-S. FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen*., 2016, f. 2, p. 315 s.

[64] Come anticipato nel Cap. I, § ?, il comma 1 dell'art. 267 c.p.p. viene progressivamente arricchito, prima dall'art. 4, comma 1, lett. *b)*, punto 1 del d.lgs. n. 216/2017 che introduce l'onere di motivazione rafforzata nel caso in cui si proceda per delitti diversi da quelli di cui all'art. 51, commi

Coerentemente con la previsione per cui l'autorizzazione a procedere deve essere calibrata sull'effettiva utilità investigativa dello strumento, la norma *de qua* è funzionale a circoscrivere la portata spazio-temporale del captatore informatico, in modo da evitare – da un lato – un'attivazione ininterrotta della spia elettronica che esporrebbe la persona controllata ad una illimitata compressione della sua riservatezza, e – dall'altro – che nel raggio d'azione della cimice itinerante incappino inopinatamente spazi domiciliari, che, come già anticipato[65], sono inviolabili quando non sussistano comprovate ragioni per ritenerli luoghi di un qualche flagrante delitto.

Un simile dispendio di energie giurisdizionali viene meno nel caso in cui si proceda per reati di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., nonchè per quelli commessi dai pubblici ufficiali e dagli incaricati di pubblico servizio contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni determinata ai sensi dell'art. 4 c.p.p., per cui, invece, l'intercettazione mediante captatore informatico «è sempre consentita»[66], senza che il decreto indichi i luoghi e i tempi dell'intrusione.

In sostanza, la nuova norma esonera il giudice dalla predeterminazione della captazione ogniqualvolta le indagini riguardino reati "distrettuali" – nonché quelli di natura economica – in considerazione del fatto che in questi casi non vi sarebbe alcun rischio di occasionali intrusioni domiciliari *contra legem.*

Eppure, anche a prescindere dalla necessità di tenere indenni dal controllo gli spazi domiciliari, una qualche determinazione degli ambiti della captazione sarebbe comunque opportuna, ai fini del sempre doveroso vaglio di utilità dell'atto intrusivo. A tal proposito, si ritiene condivisibile l'affermazione secondo cui «nessun giudice, prima dell'avvento dei *Trojan*, avrebbe autorizzato l'indiscriminata collocazione di microspie in ogni sito frequentato dal presunto mafioso, perché deve comunque esistere un nesso tra captazione della conversazione, utilità della medesima e luogo dove avviene l'intercettazione ambientale»[67]. E, infatti, pur non dovendo indicare in questi casi i luoghi e i tempi della captazione, il giudice non può essere esonerato «dall'argomentare in ordine alla necessità di eseguire la captazione in determinati ambiti […], dovendo spiegare le ragioni per cui è necessario […] disporre quella intercettazione per acquisire elementi alle indagini»[68].

Di conseguenza, la *quaestio* legata alla predeterminazione degli "spazi ambientali" oggetto di captazione e dei limiti temporali delle operazioni intercettive – vuoi per la necessità di garantire la tutela del domicilio, vuoi per garantire il rispetto del presupposto della "necessarietà" investigativa – interessa sia le operazioni da compiere in procedimenti "comuni" che in quelli "speciali".

Una volta delineata la portata della problematica concernente l'esegesi del *dictum* di cui all'art. 267, comma 1 c.p.p., l'interprete deve interrogarsi sulla fattibilità dell'imposizione prescelta dal

---

3 *bis* e 3 *quater,* c.p.p.; poi l'art. 1, comma 4, lett. *b),* l. n. 3/2019, che amplia la deroga ai delitti commessi dai pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni determinata ai sensi dell'art. 4 c.p.p. Da ultimo, l'art. 2, comma 1, lett. *d),* punto 1, d.l. n. 161/2019 prevede che un simile obbligo valga anche nel caso degli stessi delitti commessi dagli incaricati di pubblico servizio.

[65] Vedi *supra,* §?

[66] *Ex* art. 266, comma 2 *bis* c.p.p

[67] L.G. VELANI, Trojan horse, s*trumenti investigativi e diritti fondamentali: alla ricerca di un difficile equilibrio,* in *Parola alla difesa*, 2017, p. 173. Nello stesso senso P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 254 s.

[68] L'espressione appartiene a P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 254 s.

legislatore e, più correttamente, sulla possibilità di dare concreta attuazione all'onere imposto all'organo giurisdizionale.

A ben guardare, questa sagomatura del provvedimento autorizzativo si presenta nella prassi assai complicata, non solo perché l'autorità giudiziaria può relativamente "prevedere" – al momento dell'emissione del decreto – le necessità dell'indagine ma anche perché l'attuale tecnologia di funzionamento di questi *virus* spia non sembra consentire un'esecuzione davvero fedele delle prescrizioni che, secondo le nuove norme, devono accompagnare l'autorizzazione.

In altri termini, l'indicazione dei luoghi e dei tempi per cui è ammessa una simile forma intercettiva appare assolutamente incompatibile con la natura del *virus* informatico e tale impossibilità, «non dipenderebbe dalla tecnologia utilizzata, bensì dal costume sociale che caratterizza l'uso dei *device* mobili»[69]. Come evidenziato[70], il telefono cellulare – e, più in generale ogni dispositivo elettronico portatile – è, oramai, uno strumento che accompagna ogni movimento del soggetto ed è ovvio che, se usato con finalità captatorie, è in grado di operare un controllo indiscriminato della vita privata e sociale di ogni individuo, non permettendo all'autorità giudiziaria di indicare e precisare (preventivamente) i luoghi e i tempi in cui l'attività possa essere svolta, né tantomeno le categorie di soggetti che possono essere oggetto di intercettazione.

In vista delle oggettive difficoltà di delimitare gli ambienti e l'arco temporale oggetto di captazione, l'illuminato legislatore decide di introdurre un "correttivo" al sistema, prevedendo la possibilità di determinare «anche indirettamente» i luoghi e i tempi di monitoraggio[71]. Il che si traduce, sul piano empirico, nella possibilità di predisporre decreti autorizzativi alquanto vaghi e "onnicomprensivi", lasciando all'operatore l'arduo compito di individuare i momenti e gli ambienti di interesse investigativo, attivando o disattivando la microspia elettronica all'occorrenza.

A parere di chi scrive, la scelta di lasciare ai "pratici" la gestione completa delle operazioni di intercettazioni mediante *Trojan* risulta alquanto discutibile.

Intanto, una captazione che avviene solo in certi lassi di tempo predeterminati dal giudice implica notevoli difficoltà operative per l'imponente dispendio personale e – soprattutto – è difficilmente compatibile con la tecnologia di questi strumenti. Essi, infatti, non consentono sempre un ascolto sincrono, da parte di un operatore, delle conversazioni via via intercettate, in base al quale si possa agevolmente comandare da remoto l'attivazione e lo spegnimento del microfono dell'apparecchio controllato. I *software Trojan* normalmente acquisiscono i dati

---

[69] M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 44.

[70] Così, Cass., sez. VI, 26 maggio 2015, n. 27100, cit.

[71] Si legge, infatti, nella relazione di accompagnamento al d.lgs. 216/2017 che «la formula – secondo la quale nel decreto autorizzativo i luoghi e il tempo, in cui il dispositivo può essere attivato da remoto, possono essere "anche indirettamente determinati" – si spiega, dunque, nell'impossibilità di prevedere specificamente tutti gli spostamenti dell'apparecchio controllato; da qui la necessità logica di delimitare gli ambiti ai verosimili spostamenti del soggetto, in base alle emergenze investigative. A titolo esemplificativo, valga il riferimento a formule del tipo: "ovunque incontri il soggetto x"; "ogni volta che si rechi nel locale y" ecc. ecc.». Così *Relazione illustrativa*, p. 10). Anche la dottrina sul punto ha evidenziato «l'impossibilità di predeterminare con certezza gli spostamenti del supporto informatico sul quale insiste il *trojan horse*». Cfr. T. ALESCI, *Le intrusioni* inter praesentes, in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci, 2018, p. 250. Nello stesso senso C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in *www.giustiziainsieme.it*, 13 aprile 2018, p. 24 s.; M. GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore,* in *Dir. pen. cont*., 2018, f. 2, p. 40; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 219 ss.

digitali nei quali quelle conversazioni vengono tradotte, generando, ma solo periodicamente, una serie *files* audio ascoltabili dall'operatore[72].

Inoltre, seppur fosse teoricamente possibile seguire gli spostamenti del soggetto "monitorato" e, quindi, sospendere la captazione nell'ipotesi di ingresso in un luogo non autorizzato *ex* art. 267 c.p.p., «sarebbe comunque impedito il controllo del giudice al momento dell'autorizzazione, che verrebbe disposta "al buio"»[73], non consentendo all'autorità giudiziaria di esplicitare il collegamento tra mezzo investigativo e informazioni attese. Come precisato, «[S]se il giudice non determina in alcun modo dove si effettueranno le intercettazioni ambientali […] non può nemmeno motivare sull'eventualità che in tali luoghi sconosciuti possano svolgersi conversazioni utili per le indagini»[74].

Infine, una simile possibilità creerebbe non poche difficoltà in ordine al computo dei termini di durata delle intercettazioni[75], creando una netta differenza tra le intercettazioni tradizionali, le quali proseguono ininterrottamente per tutto l'arco temporale in cui sono autorizzate (normalmente 15 giorni ed eventuali successive proroghe), e quelle itineranti, i cui momenti temporali di attivazione necessitano di un apposito comando dell'autorità giudiziaria procedente[76], seppur confinati nel perimetro di durata massima dell'intercettazione[77].

L'impasse non può essere superato nemmeno ricorrendo ai dettami della giurisprudenza nazionale ed europea stratificatasi in materia di intercettazioni ambientali tradizionali che appare alquanto "flessibile" nell'imporre al giudice l'onere predeterminazione dei tempi e dei luoghi oggetto di captazione[78].

---

[72] Sul punto, S. ATERNO, *Il punto di vista degli operatori. Il difensore*, cit., p. 318 ss.; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 251; F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, cit., p. 499 s.; D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, cit., p. 576 s.; A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite virus informatico*, in AA. VV., *Le indagini atipiche*, a cura di A. Scalfati, II ed., 2019, p. 612.

[73] Cass., sez. un., 28 aprile 2016, n. 26889, cit., punto 6 motivazione.

[74] L'espressione appartiene a A. CAPONE, *Intercettazioni e costituzione*, in *Cass. pen*., 2017, f. 5, p. 1271.

[75] L'indicazione delle coordinate temporale costituisce un elemento di novità significativa, dal momento che le «limitazioni spaziali costituivano già, a seconda dei casi, patrimonio della disciplina delle intercettazioni». Così D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 221.

[76] Non bisogna dimenticare che se il *virus* informatico agisse indisturbato per tutto l'arco della giornata, il dispositivo captato andrebbe incontro a un repentino consumo di batteria e a un ingente consumo di traffico dati, così mettendo a rischio la copertura investigativa. Sul punto v. E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*, in AA. VV., Trojan horse: *tecnologia, indagini e garanzie di libertà (profili di* intelligence), in *Parola alla difesa*, 6 settembre 2016, p. 161; M. ZONARO, *Il* Trojan *– Aspetti tecnici e operativi dell'utilizzo di un innovativo strumento di intercettazione*, *ivi*, p. 166. Al contrario, secondo D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *Jusonline,* 2017, f. 3, p. 400, sarebbero proprio le operazioni di attivazione e disattivazione del microfono la causa principale di esaurimento precoce della carica della batteria del dispositivo portatile.

[77] In questo senso O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 64.

[78] Va sottolineato che né Corte EDU, Grande Camera, 4 dicembre 2015, *Roman Zakharov c. Russia*, cit., né Corte EDU., *Capriotti c. Italia*, in *Riv. it. dir. e proc. pen*., 2016, p. 1100, spesso citate per sostenere l'irrilevanza (o la non necessaria rilevanza della predeterminazione dei luoghi, nei casi in cui è ben identificata la persona o le persone controllate) si riferiscono a intercettazioni ambientali effettuate tramite *Trojan horse*.

Per quanto concerne il versante interno, la Suprema Corte, nel distinguere le intercettazioni di conversazioni e comunicazioni tra presenti da quelle telefoniche, precisa che le prime, «per loro intrinseca natura», non necessitano dell'individuazione degli apparecchi ma si riferiscono, più genericamente, ad "ambienti" in cui deve intervenire la captazione, con la conseguenza che devono considerarsi legittime, con possibilità di piena utilizzazione dei risultati, anche quando in corso di esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione[79].

D'altra parte, anche la Corte europea dei diritti dell'uomo e delle libertà fondamentali, nell'indicare i requisiti fondamentali che le legislazioni nazionali devono esibire per dirsi rispettose degli *standard* convenzionali perché un'intercettazione possa considerarsi legittima, si mostra alquanto indulgente in relazione alla specificazione del luogo di captazione. In particolare, nella già citata sentenza della Corte europea "Zakharov c. Russia", si richiede la previsione della necessaria individuazione delle persone a controllare e, solo in alternativa, la precisazione dei luoghi in cui l'intercettazione può essere effettuata[80].

---

[79] La suprema Corte mostra, dunque, un'apertura al "carattere dinamico" dell'attività di controllo, in riferimento ai diversi ambienti potenzialmente frequentabili dal soggetto ad esso sottoposto, precisando che «[S]ono utilizzabili i risultati delle intercettazioni di comunicazioni tra presenti anche quando nel corso dell'esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione, purchè rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata». In questi termini Cass., sez. II, 20 febbraio 2019, n. 19146, in *C.E.D. Cass*., n. 275583 (nella specie, la captazione ambientale era stata trasferita dalla struttura carceraria oggetto di autorizzazione ad altra struttura detentiva presso la quale l'imputato era stato successivamente tradotto); sez. V, 6 dicembre 2011, n. 5956, *ivi*, n. 252137 (la captazione ambientale era stata trasferita dalla vettura oggetto di autorizzazione ad altra vettura successivamente acquistata dall'indagato sottoposto ad intercettazione); sez. VI, 11 dicembre 2007, n. 15396, *ivi*, n. 239634 (nel caso di specie l'intercettazione di comunicazioni tra presenti aveva ad oggetto la sala colloqui della casa circondariale in cui si trovava l'imputato e le operazioni di captazione erano proseguite presso la sala colloqui della casa circondariale in cui lo stesso era stato successivamente trasferito); sez. VI, 4 settembre 2001, n. 33201, in *Dir. pen. proc*., 2001, f. 6, p. 1380 (nel caso di specie «[...] l'autorizzazione ad intercettare comunicazioni effettuate da un'utenza telefonica mobile in uso all'indagato si estende implicitamente a tutte le utenze che dal medesimo indagato risultino via via attivate mediante la prassi del cambio di scheda»); sez. IV, 11 luglio 2000, n. 4046, in *Giust. pen*., 2001, f. 2, p. 517. Inoltre la suprema Corte ha anche chiarito che «[...] l'intercettazione ambientale autorizzata in un determinato luogo è stata ritenuta legittimamente disposta anche nelle relative pertinenze». Cfr. sez. III, 15 dicembre 2010, n. 4178, in *C.E.D. Cass.,* n. 249207. Come precisato da sez. IV, 3 febbraio 2016, n. 4484, in *Proc. pen. giust*.: «[S]sono utilizzabili i risultati delle intercettazioni di comunicazioni tra presenti anche quando nel corso dell'esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione, purché tale variazione rientri nella specificità dell'ambiente oggetto dell'intercettazione autorizzata. In particolare, qualora la persona presa in osservazione abbia acquisito in uso un'altra autovettura, in sostituzione di quella indicata nel decreto autorizzativo della captazione, sussiste la medesima specificità dell'ambiente, concretamente individuato attraverso il riferimento alla frequentazione da parte di quella stessa persona fisica. Parimenti, per le intercettazioni effettuate attraverso schede telefoniche diverse da quelle originariamente utilizzate, qualora la persona nei confronti della quale l'intercettazione sia stata ritualmente autorizzata, utilizzi, per la comunicazione mediante apparecchi di telefonia mobile, schede diverse da quella per la quale l'autorizzazione sia stata disposta, non è necessario un nuovo provvedimento autorizzativo, dovendo ritenersi implicita la sua estensione a tutte le successive utenze in uso alla medesima persona». Per una ricostruzione della giurisprudenza nazionale stratificatasi in materia, P. RIVELLO, *Le intercettazioni mediante captatore informatico*, in AA. VV., *Le nuove intercettazioni*, a cura di O. Mazza, Giappichelli, 2018, p. 124 s.

[80] Corte EDU, Grande Camera, 4 dicembre 2015, *Roman Zakharov c. Russia*, cit., § 227 s.

Ma, si badi, il tutto a condizione comunque che non si autorizzino captazioni *ad explorandum*[81]: simili impostazioni giurisprudenziali, infatti, seppur tolleranti in relazione ai limiti di operatività delle intercettazioni, non giustificano affatto intercettazioni ubiquitarie, permanenti e totalizzanti, dovendo comunque il giudice preventivare le ragioni dell'atto intrusivo e i destinatari della misura[82].

Invero, una simile impostazione sembra incompatibile con la «virtuale ubiquità della cimice»[83]. Non può essere, infatti, sottaciuto che le intercettazioni tramite *Trojan* non consentono di individuare *ab origine* né i luoghi oggetto della captazione, né tantomeno le categorie di soggetti che potrebbero essere coinvolti: come rilevato, infatti, «[I]il carattere itinerante delle nuove spie elettroniche, combinato alla loro potenza d'azione, comporta il rischio di introdursi nella sfera personale di chiunque si trovi ad una certa distanza dal target, di captare fortuitamente conversazioni intercorrenti tra terzi, di penetrare in imprevedibili spazi domiciliari di chiunque (non soltanto del soggetto controllato), finanche di intercettare inopitamente su territorio estero»[84].

E nemmeno si può pensare di risolvere la *quaestio* dell'inevitabile indeterminatezza e opacità del decreto invocando rimedio dell'inutilizzabilità probatoria dei dati appresi *ultra vis*, secondo la previsione dell'art. 271, comma 1 *bis* c.p.p., dal momento un'intercettazione così condotta determina una lesione inferta illegittimamente agli interessi che le cautele esecutive in discorso mirano a salvaguardare: come evidenziato «l'inutilizzabilità, infatti, va riservata a gravi patologie degli atti del procedimento e non all'ipotesi di adozione di provvedimenti *contra legem* e non preventivamente controllabili quanto alla loro conformità alla legge»[85].

---

[81] Per comprendere meglio un tale assunto, in dottrina ha indicato il seguente esempio: «si pensi al procedimento a carico di due sodali individuati quali autori di una rapina; ottenuta l'autorizzazione all'attivazione degli ascolti mediante *trojan horse* inoculato sul dispositivo telefonico portatile di uno dei due indagati in vista dell'incontro tra i due, in area campestre, per la spartizione del profitto del reato, potrà accadere che i due interlocutori si accordino, in quella sede, anche in vista di un ulteriore "colpo" da mettere a segno in seguito, dandosi appuntamento per un nuovo incontro finalizzato alla predisposizione delle specifiche modalità operative del nuovo reato da perpetrare. In tal caso, è possibile che l'autorizzazione abbia legittimato l'intercettazione in occasione del primo incontro limitando ad esso, e ad esso solo, la facoltà di attivazione del microfono, ragione per cui il decreto del pubblico ministero che ha disposto le operazioni avrà recepito la durata complessiva limitatamente a quell'incontro, con la conseguenza che sarà necessaria una nuova autorizzazione ed un nuovo decreto in vista dell'incontro successivo. Al contrario, è possibile ipotizzare anche che il giudice abbia autorizzato, indirettamente, la captazione in ragione di ogni incontro che si svolgerà in quel luogo (o in altri luoghi) in vista di tutte le possibili occasioni d'incontro tra i due sodali: in tal caso, non sarà necessaria una nuova autorizzazione e l'ascolto avrà luogo, con attivazione del microfono ad intermittenza, ad ogni occasione d'incontro, per tutta la durata fissata con il decreto del pubblico ministero, di cui si potrà comunque disporre la proroga ad opera del giudice». D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 221 s.

[82] Cfr. Cass., sez. IV, 17 aprile 2012, n. 19618, in *Cass. pen*., 2013, f. 4, p. 1523, cono nota di G. BONO, *Il divieto di indagini ad explorandum include i mezzi informatici di ricerca della prova.*

[83] Così la definisce P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 250.

[84] P. BRONZO*, L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 339.

[85] Così L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo,* cit., p. 10. Si pensi al divieto di intercettazione dei colloqui tra il difensore e l'indagato di cui all'art. 103, comma 5 c.p.p., che, secondo l'indirizzo consolidato della Corte di cassazione, non sussiste quando le conversazioni o le comunicazioni intercettate non siano pertinenti all'attività professionale svolta dalle persone indicate nell'art. 200 c.p.p. e non riguardino di conseguenza fatti conosciuti per ragione della professione dalle stesse esercitata, sicché l'utilizzabilità valutata dopo la registrazione dei dialoghi.

Di qui, al fine di colmare *deficit* legislativi che, inevitabilmente, si ripercuotono sulla prassi investigativa ledendo i diritti dei soggetti coinvolti, la dottrina tenta di esplorare nuove rotte, fornendo soluzioni inedite per ridurre i rischi di impiego indeterminato del *virus*[86].

Secondo alcuni, bisognerebbe ipotizzare un provvedimento in cui si indichino dettagliatamente il domicilio da monitorare o la tipologia degli ambienti extradomiciliari nei quali potrà svolgersi l'intercettazione, prescrivendo l'attivazione della cimice solo quando il dispositivo infettato venga introdotto in tali luoghi[87].

In altri termini, al fine di garantire la compatibilità dell'attività con i (più blandi) contenuti del decreto autorizzativo, il captatore dovrebbe, con apposito comando inviato da remoto, essere attivato nei luoghi e per il tempo consentito dal provvedimento e disattivato nel momento in cui il dispositivo entra nelle "zone rosse", ovvero quelle estranee allo stesso. Tuttavia, seppure ciò risultasse tecnicamente possibile[88], allora si deve ammettere che il captatore non è più una mera cimice informatica ma anche uno strumento di geolocalizzazione[89], oltrepassando i limiti fattuali contemplati dalla novella che attribuisce al *virus* informatico solo la veste di una cimice ambientale[90].

Cfr. Cass., sez. VI, 17 marzo 2015, n. 18638, in *C.E.D*. Cass., n. 263548; sez. V, 25 settembre 2014, n. 42854, *ivi*, n. 261081.

[86] È stato ipotizzato, infatti, che l'autorizzazione *ex* art. 267 c.p.p. del giudice perle indagini preliminari potrebbe essere circoscritta alle conversazioni che avvengono in un luogo pubblico o aperto al pubblico. Questa condizione, evidentemente, permetterebbe il rispetto del limite allo svolgimento di intercettazioni di dialoghi tra presenti in ambienti domiciliari di cui all'art. 266, comma 2 c.p.p. Il dispositivo infettato, inoltre, potrebbe essere un p*ersonal computer* fisso o "non trasportabile", installato in un determinato posto diverso da quelli presi in considerazione dall'art. 614 c.p. ovvero in un *computer* portatile abitualmente tenuto fermo in un luogo pubblico. Più in generale, è stato evidenziato che l'agente intrusore con cui è infettato il dispositivo elettronico è controllabile a distanza; il "microfono" può essere acceso o spento a richiesta; lo *smartphone* può essere "tracciato"; in questo modo potrebbe essere evitato di procedere a registrazioni quando il portatore del telefono infettato con il programma *trojan* entra in un domicilio. In questo senso E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle sezioni unite*, in *Parola alla difesa*, 2016, 1, 161. Per una panoramica delle soluzioni offerta, L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. pen*., 2020, n. 4, p. 110 ss.

[87] F. CAJANI, *Odissea del captatore informatico,* in *Cass. pen*., 2016, f. 10, p. 4140. Una simile soluzione è suggerita anche da P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 250.

[88] Come evidenziato, «[L]la soluzione può sembrare adeguata, ma, nella maggior parte dei casi, non è risolutiva in quanto la quasi totalità degli strumenti di geolocalizzazione in commercio […] non è in grado di comprendere con esattezza se il soggetto intercettato sia in giardino, in casa, sul marciapiede o dentro un'abitazione». Così S. ATERNO, *Il punto di vista degli operatori. Il difensore*, cit., p. 330.

[89] D'altra parte, l'attivazione del geolocalizzatore è proprio la funzione che prospetta la procura di Sondrio, secondo cui «[A]appare auspicabile, al fine di evitare controversie in sede processuale, che tra i requisiti tecnici dei programmi informatici che verranno stabiliti dal Ministero della Giustizia, vi siano quelli di consentire ai programmi di accedere al sistema di localizzazione GPS […] per permettere all'operatore di identificare con certezza il luogo ove avvenga la comunicazione». Così Linee-guida della Procura di Sondrio, in *Sist. pen*., 20 gennaio 2020.

[90] Per una disamina delle funzionalità del *Trojan*, al netto della captazione di conversazioni e comunicazioni tra presenti, si rinvia a Cap. II.

5. LE IRRAGIONEVOLI LIMITAZIONI DEL POTERE DEL P.M. NELLA PROCEDURA D'URGENZA

Tra le disposizioni atte a limitare l'impiego del captatore informatico, ovvero, più correttamente, a circoscriverne l'utilizzo *sub certis verbis*, figura anche il comma 2 *bis* dell'art. 267 c.p.p., che introduce un'atipica procedura autorizzativa d'urgenza per tali forme intercettive[91].

In forza della nuova disposizione, il pubblico ministero può disporre l'intercettazione itinerante in casi di urgenza solamente se procede per uno dei delitti indicati all'art. 51, commi 3 *bis* e 3 *quater* c.p.p. e per quelli dei pubblici ufficiali e degli incaricati di pubblico servizio per i quali sia prevista la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p., con l'onere motivazionale aggiunto di indicare le ragioni di urgenza per le quali è impossibile attendere il provvedimento giudiziale.

Come evidenziato dalla dottrina, il *dictum* «desta perplessità»[92], riscontrando nello stesso anomalie interpretative e presunte violazioni ai precetti costituzionali.

In relazione al primo aspetto, il legislatore introduce una presunzione relativa di sussistenza delle situazioni d'urgenza – per le quali il pubblico ministero è legittimato a disporre la misura – per i soli delitti di criminalità organizzata (in senso stretto intesi) e per i reati di natura economica, senza, tuttavia, circoscriverne il significato, a differenza di quanto accade per le tradizionali forme di intercettazione[93]. Una simile lacuna normativa, determina il rischio di trasformare quella presunzione relativa in assoluta, ovvero far coincidere "le situazioni d'urgenza" con la sussistenza dei delitti di cui agli artt. 51, commi 3 *bis* e 3 *quater* c.p.p. e dei reati economici "gravi" commessi ai danni della pubblica amministrazione, ampliando, di fatto, i poteri del pubblico ministero e discostandosi dagli originali intenti del legislatore stesso.

Per quanto attiene alla compatibilità della normativa rispetto alle regole costituzionali, può dirsi che un primo profilo di illegittimità si ravvisa nella violazione dell'art. 76 Cost., per eccesso di delega[94].

Intanto, può rilevarsi una discrasia tra i principi direttivi del delegante e quanto effettivamente trasposto in legge dal delegato, dal momento che l'art. 267, comma 2 *bis* c.p.p. impone alla pubblica accusa di indicare «le ragioni di urgenza» che rendono impossibile attendere l'autorizzazione del giudice; al contrario, la legge delega poneva in capo al pubblico ministero un doppio onere motivazionale ben più stringente, consistente nell'indicazione delle «specifiche

---

[91] Per quanto concerne le intercettazioni tradizionali, l'art. 267, comma 2 c.p.p., prevede che nei casi di urgenza, il p.m. sia legittimato ad autorizzare il compimento delle operazioni con decreto motivato che va comunicato al g.i.p. immediatamente e comunque non oltre le ventiquattro ore dal momento dell'emissione del provvedimento; questi, entro quarantotto ore dall'adozione del provvedimento del rappresentante della pubblica accusa, decide sulla convalida con decreto motivato. Se il decreto del p.m. non viene convalidato, ovvero non viene convalidato nel termine prestabilito, l'intercettazione non può essere proseguita e i risultati di essa non possono essere utilizzati. Sul punto, *ex plurimis*, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 491 ss.; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale*, p. 1770 ss.; L. FILIPPI, sub *art. 267*, cit., p. 2622 ss.

[92] Così C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria,* cit., p. 25.

[93] Dall'esegesi del comma 2 dell'art. 267 si evince che vi è "urgenza" quando «vi è fondato motivo di ritenere che dal ritardo possa derivare un grave pregiudizio alle indagini». Tale urgenza può derivare dalla natura del reato e dal tipo di investigazioni che si vogliono adottare. *Ex multis,* Cass., sez. IV, 22 ottobre 2008, n. 45700, *in Cass. pen*., 2009, f. 11, p. 4335 ss., con nota di G. TODARO, *I requisito dell'urgenza per il decreto di intercettazione del P.M.*

[94] Così L. SURACI, Lo schema di d.lgs. di riforma della disciplina delle intercettazioni, op. cit., p. 6

situazioni di fatto che rendono impossibile la richiesta al giudice» e delle «ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini»[95].

Egualmente, si intravedono evidenti incongruenze della normativa così strutturata rispetto alle intenzioni del delegante, con riguardo alla procedura di convalida dell'autorizzazione urgente emessa dal pubblico ministero[96]. Più precisamente, l'art. 1, comma 84, lett. *e)*, n. 6, l. 103/2017 stabilisce che la convalida giudiziale debba intervenire «entro il termine massimo di quarantotto ore»; al contrario, il rinvio operato dal comma 2 *bis* dell'art. 267 c.p.p. al comma 2 del medesimo articolo dilata a settantadue ore il termine massimo in cui è atteso il provvedimento del g.i.p. In sostanza, al pubblico ministero sono concesse ventiquattro ore di tempo per comunicare al giudice per le indagini preliminari la disposizione dell'intercettazione d'urgenza, alle quali devono aggiungersi le quarantotto ore concesse a quest'ultimo per la decisione finale.

Non solo. Come evidenziano alcuni Autori[97], la *neo*-introdotta disciplina arreca un *vulnus* all'art. 3 Cost., determinando «iniqua disparità di disciplina»[98] tra il trattamento dei reati "ordinari" e dei reati "speciali" di criminalità organizzata, terroristica ed economica, legittimando il p.m. a procedere d'urgenza solo in relazione a quest'ultima categoria.

Una simile differenziazione risulterebbe «francamente irragionevole»[99], dal momento che in ogni caso al giudice per le indagini preliminari è sempre rimesso il controllo successivo sui presupposti del decreto d'urgenza.

Sulla base di quanto premesso, si ritiene che la scelta del delegato di limitare i poteri autorizzativi d'urgenza della pubblica accusa appare non solo inopportuna e inadeguata rispetto al complesso normativo di riferimento ma anche inefficace da un punto di vista investigativo.

Come anticipato, i tempi di richiesta di autorizzazione a procedere nel caso di intercettazioni tramite *Trojan* sono particolarmente lunghi e il relativo *iter* burocratico risulta assai più complesso rispetto a quello previsto per le captazioni tradizionali. E il risultato è quello di una procedura eccessivamente formalistica che mal si concilia con la eccezionalità dello strumento che, è bene ribadirlo, deve essere impiegato solo allorquando risulta "necessario" per lo svolgimento delle indagini in ragione della complessità dell'attività investigativa. Dunque, se la contingenza consente il ricorso ad un sistema così altamente sofisticato e invasivo per specifiche esigenze di indagine, parimenti deve essere concesso al p.m. un intervento rapido allorquando si intravedono ragioni di urgenza per le quali non poter attendere il provvedimento del giudicante, fermo restando l'onere per quest'ultimo procedere ad un controllo serrato del rispetto delle regole e dei presupposti del provvedimento urgente.

---

[95] Ai sensi dell'art. 1, comma 84, lett. *e*, punto 6, parte I.

[96] Secondo parte della dottrina, anche in questo caso è ravvisabile «un ulteriore profilo di contrasto» costituzionale tra la legge delega e il decreto delegato». Così L. SURACI, *Lo schema di d.lgs. di riforma della disciplina delle intercettazioni: qualche rilievo critico,* in *Quot. giur*., 5 gennaio 2018, p. 6.

[97] Cfr. O. CALAVITA, *L'odissea del* Trojan Horse. *Tra potenzialità tecniche e lacune normative*, cit., p. 72; C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria,* cit., p. 25; D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 223.

[98] Si esprime così D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, cit., p. 223.

[99] D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni* cit., p. 94.

6. IL NEBULOSO LIMITE DI OPERATIVITÀ DEL *VIRUS* NEI DELITTI DEI C.D. "COLLETTI BIANCHI". IL TRAMONTO DEL "DOPPIO BINARIO"

Discorso a parte merita la *quaestio* relativa alle investigazioni compiute mediate captatore informatico per il contrasto dei reati economici commessi dai pubblici ufficiali e dagli incaricati di pubblico servizio ai danni della pubblica amministrazione[100].

Come già chiarito in precedenza[101], la disciplina stratificatasi nel tempo risente dei cambiamenti "umorali" del legislatore contemporaneo che, nell'intento di fornire adeguate risposte all'emergenza contingente, provvede a ritoccare freneticamente la normativa *de qua*: dapprima, provvedendo a creare un modello investigativo "autonomo" per i reati corruttivi, a metà strada tra la disciplina prevista per le indagini relative ai delitti tradizionali e quella sperimentata dalla legislazione speciale per i reati di criminalità organizzata e terrorismo; poi, procedendo all'estensione del «retaggio inquisitorio»[102] del c.d. "doppio binario investigativo", equiparando, *tout court*, i reati corruttivi ai più gravi reati "distrettuali"; infine, nell'ottica di differenziare le due tipologie delittuose in ragione del principio di gradualità e proporzione, introducendo un modello "intermedio" – che differisce da quello predisposto per i reati più gravi di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p. solo in rapporto all'onere motivazionale dell'autorità giudiziaria – per i reati dei c.d. colletti bianchi.

Il risultato che ne deriva è alquanto insoddisfacente: al di là delle falle riscontrabili nella costruzione della normativa, non possono essere sottaciute le criticità sistematiche che derivano da una simile scelta legislativa.

In primo luogo, è proprio la positivizzazione del doppio binario investigativo a non convincere del tutto l'interprete. La risposta al bisogno di un efficace contrasto al fenomeno corruttivo determina un'ambigua assimilazione tra i reati di criminalità organizzata e terrorismo a quelli commessi contro la pubblica amministrazione: seppure il *trend* del legislatore sia volto alla parificazione sul piano investigativo delle fattispecie delittuose or ora richiamate[103], non può

---

[100] Sul tema, in generale, AA. VV., *Delitti dei pubblici ufficiali contro la pubblica amministrazione*, a cura di A. Marandola-B. Romano, Utet, 2020, *passim*.

[101] La normativa in materia di intercettazioni tramite captatore informatico è stata introdotta dall'art. 6 d.lgs. 216/2017, modificata dall'art. 1, commi 3 e 4, lett. *a)* e *b)* della l. n. 3/2019, l. 3 del 2019, ritoccata dall'art. 2, comma 1, lett. *f),* punto 1, d.l. n. 161/2019, per poi essere definita da art. 1, comma 1, l. n. 7/2020. Per un approfondimento della legislazione in materia, v. Cap. I, §?

[102] M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 46, secondo cui «[I]il nostro processo è inquisitorio per la parte in cui si definisce "doppio binario"; che sfrutta la "forza" di una legislazione "speciale" autoritaria e di una organizzazione investigativa mastodontica […] in cui sono ritenute "sopportabili" le limitazioni garantiste normative e giudiziarie in ragione dell'appartenenza "[anti]sociale" dell'autore del fatto».

[103] A dire il vero, il legislatore ha già assimilato la categoria dei reati contro la pubblica amministrazione a questa categoria con la l. 17 ottobre 2017, n. 161, recante "*Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, n. 159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate*", in *Gazz. uff*., 4 novembre 2017, n. 258. In particolare, la novella – che provvede a modificare il codice antimafia – inserisce gli indiziati di reati contro la pubblica amministrazione tra i soggetti sottoponibili alle misure di prevenzione personali applicate dall'autorità giudiziaria (art. 4, comma 1, lett. *i bis*, d.lgs. 159/2011). Sul punto, v. M. GRIFFO, *Il* Trojan *e le derive del terzo binario. Dalla riforma Orlando al d.l. 161/2019, passando per la "spazzacorrotti" e il decreto sicurezza* bis, cit., p. 67.

sottacersi come la comune prospettiva economica tra le due forme criminogene «non comport[i] identità di fatti né di discipline processuali […]»[104].

Come rilevato, «[L]le associazioni per delinquere, sia di stampo mafioso che non, […] presentano una dimensione fisica-spaziale di fondamentale rilievo, che si traduce in concreto sia in manifestazioni più eclatanti come il controllo in forma anti-statale di porzioni di territorio, tramite un sistema di squadre, di picchetti e di vedette, sia in operazioni dal carattere più occulto, come la costruzione di fortilizi o la strutturazione di edifici in modo da favorire costantemente la fuga e il nascondimento degli uomini di spicco delle cosche, o la scelta di interlocutori istituzionali apparentemente insospettabili»[105]. In questi casi, le intercettazioni virali rappresentano uno strumento indispensabile non solo per la raccolta di prove ma anche per l'identificazione, la localizzazione e la cattura dei soggetti attivi.

Viceversa, i fenomeni corruttivi, «consistendo il loro nucleo in una sorta di "contratto a causa illecita" – o *pactum sceleris* – fra il pubblico ufficiale e il suo corruttore, sia esso istantaneo (corruzione in atti) o di durata […], funzionale all'esercizio distorto del potere amministrativo, non presentano una dimensione fisica altrettanto pervasiva connessa alla vita e al funzionamento dell'accordo stesso»[106]. In questi casi, seppure le comunicazioni fra corrotto e corruttore tendono a muoversi lungo reti connotate da riservatezza e da rapporti personali diretti – e, di conseguenza, le captazioni a mezzo *Trojan* risulterebbero maggiormente efficaci nella persecuzione dell'illecito –, si ritiene che non si possa (e non deve) giustificare di per sé il ricorso a mezzi di ricerca della prova ancor più invasivi per la vita del singolo[107], perchè «[N]non tutto si può fare in nome dell'efficacia»[108].

In altri termini, una simile scelta - funzionale a facilitare e migliorare la qualità delle indagini - contribuisce ad acuire quella prassi deviata per cui il regime derogatorio di cui all'art. 13 del d.l. 152/1991, inizialmente limitato ai soli delitti di criminalità organizzata e terroristica e poi ampliato a numerose altre categorie delittuose, diventi la "norma", una regola[109].

Come rilevato, l'appiattimento del legislatore sul modulo di cui all'art. 13, d.l. 152/1991 conferma la deriva verso modalità intercettive ben lontane dall'offrire quel necessario ragionato bilanciamento tra esigenze investigative e diritti fondamentali che l'atto richiederebbe anche a seconda dei reati interessati"[110], facendo perdere al sistema la sua caratteristica intrinseca della

---

[104] Così M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 31. ID., *Rilievi sull'impiego del* trojan *nei procedimenti per i reati contro la pubblica amministrazione*, in *Proc. pen. giust.*, 2020, n. 2, p. 284.

[105] Si esprimono così F. Camplani-O. Calavita, *L'estensione dell'utilizzo del captatore informatico ai reati di corruzione: una prima lettura,* in *Ist. dir. economia*, 2019, f. 1, 7.

[106] F. Camplani-O. Calavita, *L'estensione dell'utilizzo del captatore informatico ai reati di corruzione: una prima lettura,* cit., 8.

[107] In questo senso R. Cantone– E. Carloni, *Corruzione e anticorruzione. Dieci lezioni,* Roma-Bari, 2018, 67 ss.

[108] R. Orlandi, *L'emergenza figlia delle garanzie? Riflessioni intorno alle norme e alle pratiche di contrasto alla mafia e al terrorismo,* cit.

[109] In questo senso F. RUGGIERI, *Le deroghe alla disciplina codicistica, in* AA. VV., *L'intercettazione di comunicazioni*, cit., p. 108. Come precisa S. FURFARO, voce *Intercettazioni (profili di riforma),* cit., p. 7 s., «lo statuto delle intercettazioni relative alle indagini concernenti la criminalità organizzata, pur ponendosi evidentemente come legge speciale (*ratione materiae*) rispetto alla disciplina codicistica, ha assunto connotazioni tali che può pacificamente affermarsi, non solo che su di esso si è affermata (e quotidianamente si conferma) la prassi, ma che proprio le disposizioni *ivi* previste si pongono come canoni di riferimento degli interventi normativi in tema dei presupposti e di controlli. Secondo un procedere di progressiva estensione del particolare, si sta realizzando la stabilizzazione di tutta quanta la materia delle intercettazioni su ciò che è meno garantito».

[110] Così F. RUGGIERI, *Le deroghe alla disciplina codicistica*, cit., p. 108.

gradualità del trattamento riservato all'accertamento dei fatti di reato e al giudizio, tendendo ad un'equiparazione tra fattispecie di differente gravità[111].

Una simile scelta produce conseguenze processuali di non poco conto, dal momento che si «autorizza l'interprete alla ricerca delle condizioni di ammissibilità guardando a qualunque reato che, seppur estraneo al numero chiuso che compone la categoria […] abbia quei soggetti attivi e sia lesivo di interessi riconducibili alla pubblica amministrazione»[112], con il precipuo intento di ampliare l'ambito applicativo dello strumento in assenza di una chiara indicazione di campo da parte del legislatore.

In secondo luogo, la normativa così come congegnata acuisce la confusione esegetica nell'interprete circa il *modus operandi* da adottare nel caso concreto: la riconducibilità alla criminalità mafiosa dei delitti dei colletti bianchi non deve, infatti, far impropriamente ritenere che sia venuta meno una disciplina "intermedia" che continua a vigere in relazione ai procedimenti comunque facenti capo ad un'associazione per delinquere che non rientrano nei reati distrettuali espressamente richiamati dall'art. 266, comma 2 *bis* c.p.p.

In effetti, tentando una schematizzazione, si può sostenere che allo stato esiste una disciplina "triparita" in materia di captazioni mediante *Trojan*: 1) da una parte, vi sono i reati distrettuali di cui all'art. 51 commi 3 *bis* e 3 *quater* c.p.p., per cui sono sempre consentite le intercettazioni ambientali domiciliari; 2) dall'altra, vi sono i reati "comuni", per i quali, invece, l'impiego dello strumento soggiace ai limiti di cui al comma 2 del medesimo articolo; 3) infine, esiste una normazione anomala in relazione ai procedimenti facenti capo a un'associazione per delinquere seppur diversa dalle fattispecie contemplate dall'art. 51, commi 3 *bis* e -*quater,* c.p.p.[113] – nonché quelli la cui disciplina risulta equiparata all'art. 13 del d.l. n. 152/91[114] – per i quali, invece, pur non essendo previsto un limite all'intrusione domiciliare, non trova applicazione né la disciplina più estensiva del nuovo comma 2 *bis* dell'art. 266 c.p.p. né le altre disposizioni derogatorie di cui all'art. 267, comma 1 e 2 *bis* c.p.p.

Ma c'è di più. Dal combinato disposto degli artt. 266, comma 2 *bis* e 267, comma 1 c.p.p., si evince una quarta categoria "ibrida" che si accomuna (senza sovrapporsi) ai delitti di mafia e

---

[111] Sul tema F. RUGGIERI, *Diritto processuale e pratiche criminali*, Zanichelli, 2018, p. 167 ss. Nello stesso senso G. TABASCO, *Intercettazioni, a mezzo di captatore informatico, nei procedimenti per i delitti contro la pubblica amministrazione*, in AA. VV., *La legge anticorruzione 9 gennaio 2019, n. 3*. Aggiornata alla l. 28 giugno 2019, a cura di M. Del Tufo, Giappichelli, 2019, p. 153 ss.; S. SIGNORATO, *Intercettazioni di comunicazioni*, in AA. VV., *Una nuova legge contro la corruzione. Commento alla legge 9 gennaio 2019, n. 3*, a cura di R. Orlandi-S. Seminara, Giappichelli, 2019, p. 245 ss. Secondo R. RAMPIONI, *Captatore informatico e delitti dei pubblici ufficiali contro la P.A. Le Sezioni unite civili riconoscono, in modo erroneo, la immediata applicabilità della legge cd. "Spazzacorrotti*", in *Arch. pen.*, 2020, n. 1, p. 9, «[N]non può […] difettare un rapporto di proporzionalità diretta fra il grado di intrusività della specifica misura e il livello di intensità delle garanzie legali, attraverso un equilibrato bilanciamento tra contrapposti "valori" di rilevanza costituzionale».

[112] G. SANTALUCIA, *Il diritto alla riservatezza,* cit., p. 58.

[113] Si tratta, più precisamente, dei procedimenti facenti capo ad un'associazione per delinquere, *ex* art. 416 c.p., correlate alle attività criminose più diverse, con esclusione del mero concorso di persone nel reato, per cui si applicano le disposizioni di cui all'art. 13, d.l. n. 152/91 in forza di quanto indicato da Cass., sez. un., 28 aprile 2016, n. 26889, cit. Sul punto, si veda D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 92.

[114] Il riferimento è all'art. 9 l. 11 agosto 2003, n. 228 che estende l'applicazione delle disposizioni di cui all'art. 13 d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, dalla l. 12 luglio 1991, n. 203, in relazione ai procedimenti per i delitti previsti dal Libro II, Titolo XII, Capo III, Sez. I c.p. (al netto delle ipotesi ricomprese nell'art. 51, comma 3 *bis*, c.p.p.), nonché a quelli previsti dall'art. 3, l. 20 febbraio 1958, n. 75.

assimilati. Più precisamente, si prevede che il decreto autorizzativo con il quale l'autorità giudiziaria acconsente alle intercettazioni ambientali domiciliari per i delitti "gravi" di criminalità economica, debba indicare non solo le ragioni per che rendono necessario l'impiego della nuova tecnica intercettiva ma anche i motivi che ne giustificano l'utilizzo nei luoghi dell'art. 614 c.p., differenziando ulteriormente la disciplina *de qua* rispetto a quella prevista per i reati distrettuali. In altri termini, per i reati corruttivi, pur non essendo previsti limiti alle intrusioni nei luoghi di cui all'art. 614 c.p., devono sussistere specifiche ragioni che ne giustificano l'impiego anche in un simile ambiente e che, si badi, non coincidono con la dimostrazione del fondato motivo di ritenere che in quei luoghi si stia svolgendo un'attività criminosa[115].

Prima facie, la scelta di aggravare l'onere motivazionale del decreto autorizzativo sembra determinare un regime ancor più speciale e selettivo che tende a differenziare tali fattispecie di reato da tutte le altre categorie delittuose. Tuttavia, la previsione in parola, seppur funzionale ad operare una distinzione tra le due differenti forme di criminalità nell'ottica di una gradualità della gravità, finisce per rappresentare solo un mero esercizio di stile che contribuisce ad acuire quelle difficoltà e quei dubbi applicativi che già prima della riforma del 2020 apparivano insormontabili. A ben guardare, infatti, il requisito dell'"utilità" dell'intrusione domiciliare, non configura quale presupposto di ammissibilità; cosicchè l'eventuale omessa indicazione delle suddette ragioni non sconta certamente la sanzione di inutilizzabilità dei risultati, di cui al primo comma dell'art. 271 c.p.p., in quanto non eseguita al di fuori dei *casi* consentiti dalla legge.

Di qui, può ritenersi che l'innesto normativo, di scarso impatto innovativo, sia servito solo quale *escamotage* governativo per sedare il malcontento di coloro che avevano intravisto nelle scelte legislative pregresse di consentire senza limiti spazio-temporali l'impiego del virus anche per tali fattispecie di reato un «attentato al sistema»[116].

6.1. *SEGUE*: QUESTIONI DI DIRITTO INTERTEMPORALE. IL TERMINE INIZIALE DI EFFICACIA DELLE NUOVE DISPOSIZIONI

Altro profilo critico della disciplina relativa all'impiego del captatore informatico quale strumento di contrasto al fenomeno corruttivo, inerisce all'entrata in vigore delle disposizioni riformate che, pur risultando formalmente efficaci, non trovano ancora alcuna compiuta realizzazione in quanto innestate in un testo mai attuato.

Per poter meglio comprendere i termini della questione, occorre ripercorrere brevemente le tappe salienti delle modifiche legislative intervenute in materia.

Come noto, le disposizioni del d.lgs. 216/2017 sull'uso del *Trojan* per l'intercettazione tra presenti non hanno ancora acquistato efficacia a seguito di numerosi rimbalzi legislativi che ne hanno posposto l'attuazione[117]. Unica eccezione alla regola è rappresentata dalle previsioni

---

[115] Come precisato, «[È]è da ritenere che, per consentire l'attivazione del microfono nei luoghi di privata dimora, la giustificazione richiesta dalla norma non è solo quella rappresentata dal fondato motivo di ritenere che *ivi* si stia svolgendo un'attività criminosa, ma è rinvenibile in qualsivoglia altra spiegazione [condivisa dal giudice] a supporto della necessità dell'attivazione del microfono nel domicilio o in altro luogo privato: ad esempio, basterebbe la rappresentazione del fatto che in tali luoghi possano rinvenirsi elementi probatori essenziali, perché solo o principalmente in tali luoghi l'apparecchio "infettato" viene utilizzato». Così Linee-guida della procura della Repubblica di Bologna, *La nuova disciplina delle intercettazioni. Profili di interesse per l'Ufficio del pubblico ministero*, in *www.procura.bologna.giustizia.it,* 11 marzo 2020

[116] M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., p. 55.

[117] V. *supra* § 1.

contenute nell'art. 6 del decreto, con il quale si è data attuazione alla direttiva per la «semplificazione delle condizioni per l'impiego delle intercettazioni […] nei procedimenti per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione»[118], che, per espressa previsione normativa, trovano attuazione contestualmente all'entrata in vigore della novella[119].

Su questo impianto, interviene la legge n. 3 del 2019 che (oltre a rendere sempre possibili le intercettazioni ambientali con il captatore informatico per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione) abroga la norma che vieta l'effettuazione delle captazioni tramite *Trojan* nei luoghi di privata dimora in assenza di motivi per ritenere in corso attività criminosa.

Di qui, le perplessità, dal momento che l'abrogazione del comma 2 dell'art. 6 del d.lgs. 216/2017, a differenza della norma codicistica di innovazione, non è stata sottoposta ad alcun termine di efficacia ed è dunque divenuta formalmente operativa con l'entrata in vigore della legge, ossia il 31 gennaio 2019.

Il quesito che a questo punto si pone è se tale abrogazione abbia comportato con effetto immediato, ossia dall'entrata in vigore dell'abrogazione, la piena assimilazione delle discipline nei due diversi ambiti procedimentali. Se cioè, a far data dall'abrogazione – e non dal momento in cui acquisteranno efficacia le disposizioni codicistiche – l'equiparazione voluta dalla legge Spazzacorrotti tra procedimenti di criminalità mafiosa e terroristica e procedimenti per delitti contro la pubblica amministrazione sia divenuta operativa[120].

Sul punto, la dottrina è assai confusa, potendosi intravedere due schieramenti antitetici[121]: c'è chi[122] sostiene che il captatore informatico sia utilizzabile per le indagini relative ai reati dei pubblici ufficiali contro la pubblica amministrazione già dal 26 gennaio 2018, ovvero dalla data

[118] Cfr. art. 1, comma 84, lett. *d*, l. n. 103/2017.

[119] E, quindi, dal 26 gennaio 2018.

[120] Sul tema L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte,* cit., p. 109 ss.; G. SANTALUCIA, *Delitti dei c.d. colletti bianchi e intercettazioni tra presenti su dispositivo portatile: termine iniziale di efficacie delle nuove disposizioni. Spunti dalla sentenza n. 741 delle Sezioni unite civili,* cit., p. 6 s.

[121] Per una ricostruzione delle posizioni dottrinali, L. GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte,* cit., p. 109 ss.

[122] Sostengono una simile posizione L. GIORDANO, *Il ricorso al "captatore informatico" nelle indagini per i reati contro la pubblica amministrazione,* in AA. VV., *La nuova disciplina dei delitti di corruzione. Profili penali e processuali*, a cura di G. Flora-A. Marandola, Pacini, 2019, p. 90 ss.; C. PARODI, *Intercettazioni. Come è (ri)cambiata la disciplina dopo i decreti sicurezza e anticorruzione*, in *Il Penalista*, 25 gennaio 2019.

di entrata in vigore del decreto 216/2017[123] e chi[124], per converso, ritiene che la disciplina *de qua* segua inevitabilmente le sorti della riforma nel suo complesso, dovendo la sua attuazione attendere l'operatività delle disposizioni generali sull'uso del captatore informatico.

A sostegno della piena vigenza della normativa, è stato rilevato che «la disposizione transitoria dell'art. 9 del d.lgs. 216/2017 non contemplava l'art. 6, che, pertanto, è da tempo in vigore. […] Inoltre, con la l. 3/2019, è stato abrogato il comma secondo del citato art. 6 – che limitava le "potenzialità" contenute nel comma 1 – così che oggi la disciplina delle intercettazioni in tema di reati di p.a. è equiparata in tutto a quella in tema di criminalità organizzata e terrorismo. Ne consegue che, in attesa della piena operatività delle disposizioni generali sull'uso del captatore, l'esecuzione di tali forme di captazioni in tema criminalità organizzata, terrorismo e p.a. non potranno che essere valutate e eseguite in conformità alle indicazioni del testo originario degli artt. 266 e 267 c.p.p. sulla base delle indicazioni della Suprema Corte»[125].

Tale impostazione sembra essere prescelta anche dalla giurisprudenza civile (e, in maniera meno netta, da quella penale)[126], la quale legittima l'impiego processuale dei risultati intercettivi

---

[123] Più precisamente: 1) a far data dal 26 gennaio 2018, epoca di entrata in vigore dell'art. 6 del d.lgs. n. 216 del 2017, deve ritenersi ammissibile il ricorso al captatore informatico per le intercettazioni tra presenti nelle indagini per i reati dei pubblici ufficiali contro la pubblica amministrazione, in forza del rinvio all'art. 13 d.l. n. 152 del 1991, come interpretato dalla sentenza delle Sezioni unite "Scurato", contenuto nell'art. 6, comma 1, d.lgs. n. 216 del 2017; 2) dal 31 gennaio 2019, epoca di entrata in vigore della legge n. 3 del 2019, è ammissibile l'impiego dello strumento in esame, per i reati indicati, anche in luoghi domiciliari e in carenza della prova che sia in corso l'attività criminosa in forza: a) dell'art. 6, comma 1, del d.lgs. n. 216 del 2017, che dispone l'applicazione delle disposizioni di cui all'art. 13 del d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203 ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni; b) dell'art. 1, comma 3, della legge n. 3 del 2019 che, abrogando l'art. 6, comma 2, del d.lgs. n. 216 del 2017, ha permesso l'applicazione a tali procedimenti anche dell'ultima parte dell'art. 13, comma 1, del d.l. n. 152 del 1991; c) dei principi espressi da Cass., sez. un., 28 aprile 2016, n. 26889, cit., che, nei procedimenti soggetti alla disciplina di cui all'art. 13 del d.l. n. 152 del 1991, ha ritenuto ammissibile l'utilizzo del captatore informatico per realizzare intercettazioni tra presenti.

[124] In dottrina, si veda L. FILIPPI, *Riforme attuate, riforme fallite e riforme mancate degli ultimi 30 anni. Le intercettazioni*, in *Arch. pen*., 2019, f. 3, p. 41 ss., secondo cui «la circostanza che ad essi (ai procedimenti per i reati dei pubblici ufficiali contro la pubblica amministrazione) si applichino, in ragione dell'art. 6, comma 1, d.lgs. n. 216 del 2017, le regole dettate dal citato art. 13, non pare idonea a determinare un'estensione in *malam partem* del *dictum* della menzionata pronuncia (la sentenza Scurato)»; S. SIGNORATO, *Intercettazioni di comunicazioni*, cit., p. 255 ss. secondo cui «essendo stata prorogata l'entrata in vigore della norma contenitore (artt. 266 e 267 c.p.p.) risulta automaticamente prorogato anche il (variato) contenuto», mentre l'abrogazione dell'art. 6, comma 2, del d.lgs. n. 216 del 2017 si limita a semplificare presupposti e condizioni per effettuare le intercettazioni di conversazioni o comunicazioni per i reati dei pubblici ufficiali contro la pubblica amministrazione con mezzi diversi dal *trojan*. Nello stesso senso M. GRIFFO, *Il captatore informatico e la filosofia del doppio binario*, cit., 391 ss.; R. RAMPIONI, *Captatore informatico e delitti dei pubblici ufficiali contro la P.A. Le Sezioni unite civili riconoscono, in modo erroneo, la immediata applicabilità della legge cd. "Spazzacorrotti"*, cit., p. 3 s.; G. SANTALUCIA, *Delitti dei c.d. colletti bianchi e intercettazioni tra presenti su dispositivo portatile: termine iniziale di efficacie delle nuove disposizioni. Spunti dalla sentenza n. 741 delle Sezioni unite civili,* cit., p. 6 s.

[125] Così C. PARODI, *Intercettazioni. Come è (ri)cambiata la disciplina dopo i decreti sicurezza e anticorruzione*, cit.

[126] Cass., sez. I, 25 giugno 2019, n. 50972, in *C.E.D. Cass*., n. 27786. In questa pronuncia, la Corte affronta marginalmente il tema, procedendo ad una ricostruzione del quadro delle recenti modifiche normative in punto di intercettazioni tra presenti a mezzo di captatore su dispositivo elettronico portatile. Dopo aver osservato che con l'inserimento di una ulteriore previsione al comma 2 *bis*

ottenuti mediante l'ausilio di captatore informatico in un procedimento disciplinare riguardante dei magistrati[127].

Sul versante opposto, si ritiene che il differimento dell'applicazione del captatore informatico disposto dall'art. 9 del d.lgs. n. 216/2017, avrebbe un preciso fondamento, trovando la sua ragion d'essere nella necessità di sopperire a difficoltà di ordine fattuale. Come si evince dalla lettura della relazione illustrativa al d.lgs. 216/2017, infatti, il rinvio è funzionale a «consentire ai singoli uffici di dettare le opportune indicazioni funzionali a dare attuazione al nuovo sistema di archivio riservato, sì da assicurare effettività di tutela del segreto su quanto ivi custodito e, dunque, per offrire le più adeguate tutele per ovviare al rischio di causare sacrifici eccessivi ed evitabili ai diritti delle persone coinvolte»[128].

Nello stesso senso anche i successivi interventi legislativi che prorogano l'entrata in vigore della novella che giustificano il rinvio con la necessità di «adeguare nel modo migliore le attività e le misure organizzative rispetto alle necessità degli uffici», in modo da aver certezza di «giungere all'operatività piena della disciplina con le misure organizzative completamente dispiegate e funzionanti»[129].

Dunque, «non sembra eccessivo concludere che sarebbe contrario al senso della strategia normativa l'assunto secondo cui dall'abrogazione della disposizione che chiariva l'impossibilità di una piena assimilazione dei regimi di disciplina tra i procedimenti per criminalità organizzata e procedimenti per delitti dei pubblici ufficiali [e degli incaricati di pubblico servizio] contro la pubblica amministrazione discenderebbe per questa ultima categoria di procedimenti l'immediata possibilità d'uso dello strumento investigativo, seppure per essi la previsione del codice di equiparazione – al fine specifico dell'uso del *Trojan* in dispositivo portatile per l'intercettazione

---

all'art. 266 c.p.p. si prevede la possibilità, senza ulteriori condizioni, dell'intercettazione tra presenti a mezzo captatore e su dispositivo portatile anche nei procedimenti per delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore a cinque anni determinata ai sensi dell'art. 4 c.p.p., aggiunge che la disposizione «si applica alle operazioni di intercettazione relative a provvedimenti di autorizzazione emessi dopo il 31 dicembre 2019». Tuttavia, sottolinea la Corte, «ai procedimenti per delitti dei pubblici ufficiali contro la pubblica amministrazione si applica, per effetto dell'art. 6 d. lgs. n. 216 del 2017, la disciplina dell'art. 13 d. l. n. 152 del 1991 e successive modificazioni», con la conseguenza «che il rinvio alla norma anzidetta renderebbe a regime la nuova disciplina e di operatività immediata il relativo statuto regolatore».

[127] Come sostenuto, «nel procedimento disciplinare riguardante i magistrati sono utilizzabili le intercettazioni effettuate in un procedimento penale, anteriormente al 1 gennaio 2020, con captatore informatico […] su dispositivo mobile nella vigenza ed in conformità della disciplina introdotta dall'articolo 6 del d.lgs. n. 216 del 2017 (che ha parzialmente esteso ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione, puniti con la pena della reclusione non inferiore nel massimo a cinque anni, la disciplina delle intercettazioni prevista per i delitti di criminalità organizzata dall'articolo 13 del d.l. n. 152 del 1991, conv., con modif., dalla l. n. 203 del 1991 ed integrato con d.l. n. 306 del 1992, conv., con modif., dalla l. n. 356 del 1992) e dall'articolo 1, comma 3, della l. n. 3 del 2019 (la quale, abrogando il comma 2 dell'articolo 6 del citato d.lgs. n. 216 del 2017, ha eliminato la restrizione dell'uso del captatore informatico nei luoghi indicati dall'articolo 614 c.p., così consentendo l'intercettazione in tali luoghi anche se non vi è motivo di ritenere che vi si stia svolgendo attività criminosa), atteso che la prima di tali norme, non rientrando tra quelle per le quali l'articolo 9 del medesimo d.lgs. n. 216 del 2017 ha disposto il differimento dell'entrata in vigore, è efficace dal 26 gennaio 2018, mentre la seconda (a differenza di altre disposizioni della medesima legge per le quali il legislatore ha differito l'entrata in vigore al 1° gennaio 2020) è efficace dal decimoquinto giorno dalla pubblicazione della legge sulla Gazzetta Ufficiale, avvenuta il 16 gennaio 2019». Così Cass., sez. un., 15 gennaio 2020, n. 741, in *C.E.D. Cass.*, n., 656792.

[128] Così *Relazione illustrativa*, cit., p. 12.

[129] Così *Relazione tecnica di accompagnamento al disegno di legge riguardante la conversione del d.l. 161/2019*, reperibile al sito *www.senato.it*.

tra presenti – ai procedimenti per delitti di mafia e di terrorismo sia oggetto espresso della previsione di rinvio»[130]. D'altra parte, ove il legislatore avesse inteso aprire all'immediato uso del captatore informatico per l'intercettazione tra presenti in ambito domiciliare nei procedimenti contro la pubblica amministrazione, avrebbe dotato anche questa previsione di garanzia di una pari immediata efficacia, invece che differirne l'operatività nel tempo al pari delle altre disposizioni del decreto legge n. 161 del 2019, e correlativamente di quelle del d.lgs. 216/2017.

Infine, sarebbero ragioni di coerenza sistemica a giustificare un simile approccio: se nessuna norma in materia di intercettazioni mediante virus informatico trova compiuta realizzazione, nemmeno la disciplina "speciale" prevista per i delitti dei c.d. colletti bianchi può trovare impiego, pena la disparità di trattamento dei soggetti coinvolti, determinando una violazione del principio di eguaglianza formale e sostanziale di cui all'art. 3 Cost.

Pur condividendo le argomentazioni addotte a sostegno del differimento di entrata in vigore di tali disposizioni, l'approdo ermeneutico raggiuto appare all'interprete non pienamente soddisfacente, peccando di un certo rigorismo. Il sistema costituito, infatti, sembra offrire spazi per una diversa ricostruzione della disciplina *de qua*: adottando una posizione intermedia, meno netta tra le due impostazioni richiamate, si potrebbe ritenere che solo la disposizione contenuta nel primo comma dell'art. 6, d.lgs. 216/2017 (ossia quella riguardante l'estensione alle "ordinarie" intercettazioni dell'art. 13, d.l. 152/1991 nei procedimenti per i più gravi delitti di corruzione) sia entrata in vigore il 26 gennai 2018; viceversa, quella contenuta nel secondo comma (poi abrogata e riformulata dalla l. 3/2019), non contenendo una previsione dotata di una propria autonomia, «risulta necessariamente destinata a combinarsi con la norma che ammette […] l'uso dei captatori informatici [ossia] l'art. 266, comma 2 c.p.p.»[131]. Se ne ricava che la disciplina in esame non può trovare applicazione immediata, subendo il differimento previsto per le disposizioni della legge Orlando, dovendo, per converso, dare esecuzione alla regolamentazione previgente[132].

7. GLI USI OBLIQUI A FINI INVESTIGATIVI. IL SUPERAMENTO DEI LIMITI DI INUTILIZZABILITÀ PROCEDIMENTALE NELLA L. 7/2020

Nel *genus* delle norme atte a potenziare gli effetti delle investigazioni tramite *Trojan*, figurano quelle disposizioni relative alla spendibilità processuale dei risultati acquisiti mediante captatore, dalle quali discendono le maggiori perplessità degli interpreti a fronte di un ingiustificato ampliamento dei casi di impiego "trasversale" dei dati e delle informazioni così apprese.

Come già anticipato[133], il comma 1 dell'art. 270 c.p.p., rimasto immune ai ritocchi normativi pregressi, subisce una modifica ad opera della l. 7/2020 sotto un duplice profilo: da un lato, si rafforzano le condizioni che legittimano l'impiego dei risultati captativi in procedimenti diversi da quelli indicati nel decreto autorizzativo, attraverso l'introduzione del requisito della rilevanza

---

[130] G. SANTALUCIA, *Delitti dei c.d. colletti bianchi e intercettazioni tra presenti su dispositivo portatile: termine iniziale di efficacie delle nuove disposizioni. Spunti dalla sentenza n. 741 delle Sezioni unite civili,* cit., p. 11.

[131] Si esprime così R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, f. 2, p. 560.

[132] Va precisato che in materia non esisteva alcuna regola *ad hoc,* per cui la normativa previgente è quella stabilita in via giurisprudenziale, in particolare dalla presa di posizione della Corte di cassazione a sezioni unite nella già citata sentenza Scurato. In questo senso, R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 561.

[133] Cfr. Cap. I, § ?.

che completa l'indispensabilità investigativa[134]; dall'altro, viene introdotta un'ulteriore ipotesi derogatoria al regime di inutilizzabilità, prevedendo che la trasmigrazione del captato possa considerarsi legittima non solo per l'accertamento dei delitti per i quali l'arresto in flagranza è obbligatorio, ma anche dei reati di cui all'art. 266, comma 1 c.p.p.[135].

Pochi ritocchi lessicali per una modifica (s)travolgente.

Per comprendere appieno una simile affermazione appare imprescindibile riferirsi al mutato contesto giurisprudenziale in cui si insinua la novella. Qualche mese prima dell'intervento riformatore, infatti, le Sezioni unite della Suprema Corte si pronunciano sul tema *de qua*[136], al

---

[134] Come precisato, «[…] è ovvio che ciò che è "indispensabile" deve necessariamente essere anche "rilevante". […] L'impiego della congiunzione "e" significa che il legislatore ha voluto indicare due requisiti tra loro cumulativi, per cui l'utilizzazione nel diverso procedimento deve ritenersi ammessa solo se indispensabile per un reato per il quale l'art. 266, comma 1, c.p.p. ammette l'intercettazione e per il quale sia inoltre imposto l'arresto obbligatorio in flagranza (art. 270, comma 1, c.p.p.). Se invece la disposizione fosse intesa come se ammettesse l'utilizzabilità per qualsiasi reato suscettibile di intercettazione, sarebbe incostituzionale in rapporto alla prescrizione, dettata dall'art. 15 Cost., dell'"atto motivato dell'autori giudiziaria" e rappresenterebbe un'inammissibile "autorizzazione in bianco" ad intercettare […]». Così L. FILIPPI, *Intercettazioni:* habemus legem!, cit., p. 462.

[135] L. n. 7/2020, che modifica l'art. 2, comma 1, lett. *g)*, d.l. n. 161/2019, attraverso l'interpolazione di un nuovo punto "01". Per un primo commento, A. MARANDOLA, *Intercettazioni: una riforma nel segno della "non dispersione". I nuovi limiti di utilizzabilità* ex *art. 270 c.p.p.,* in *il Penalista,* 24 febbraio 2020.

[136] Cfr. Cass., sez. un., 28 novembre 2019, n. 51, in *Guida dir*., 2020, f. 6, p. 79 ss., con nota di A. NATALINI, U*so obliquo dei flussi: vaglio d'ammissibilità sempre necessario*; in *Cass. pen*., 2020, f. 5, p. 1877, con nota di K. NATALI, *Sezioni Unite e "Legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*. Sul tema, anche, F. ALVINO, Bene captum, male retentum: *riflessioni in merito all'art. 270 c.p.p., in materia di circolazione endoprocedimentale delle intercettazioni, e a margine delle sezioni unite Cavallo,* in *Il dir. vivente*, 18 gennaio 2020; G. ILLUMINATI, *Utilizzazione delle intercettazioni in procedimenti diversi: le sezioni unite ristabiliscono la legalità costituzionale*, in *Sist. pen.*, 30 gennaio 2020; A. INNOCENTI, *Le sezioni unite limitano l'utilizzabilità dei risultati delle intercettazioni per la prova di reati diversi da quelli per cui sono state ab origine disposte*, in *Dir. pen. proc.,* 2020, n. 7, p. 993 ss.; F. VANORIO, *Il permanente problema dell'utilizzo delle intercettazioni per reati diversi tra l'intervento delle Sezioni Unite e la riforma del 2020*, *ivi,* 12 giugno 2020. Sul punto anche G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., p. 143 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 102 ss.

fine di dare riposta all'annosa *querelle* che imperversa in dottrina[137] e in giurisprudenza[138].

In quell'occasione, la Corte chiarisce la portata del dettato di cui all'art. 270, comma 1 c.p.p., prevedendo che il divieto in esame non operi, oltre che nel caso di reati successivamente emersi che siano ricompresi tra quelli per cui è previsto l'arresto obbligatorio in flagranza, anche con riferimento ai risultati relativi ai reati che sono connessi *ex* art. 12 c.p.p.[139], sempre che rientrino

---

[137] Sul tema dell'utilizzabilità delle intercettazioni in altro procedimento, si vedano, tra i tanti, E. APRILE, *Intercettazioni di comunicazioni*, cit., p. 482; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, cit., p. 203 ss.; V. CANTONE, *L'utilizzazione delle intercettazioni telefoniche in "procedimenti diversi"*, in *Cass. pen.,* 1997, f. 5, p. 1431 ss.; F. G. CAPITANI, *La Cassazione detta il* vademecum *per l'utilizzo delle intercettazioni in procedimenti diversi*, in *Dir. e giust*., 2016, f. 4, p. 30 ss.; M. S. CHELO, *Il procedimento "diverso*" ex *art. 270 c.p.p. ovvero la portata del divieto di utilizzabilità delle intercettazioni telefoniche*, in *Il Penalista*, 17 marzo 2016; M. CIAPPI, *Limiti all'utilizzabilità delle intercettazioni provenienti* aliunde, in *Dir. pen. proc.,* 1996, f. 6, p. 1242 ss.; C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema,* in *Cass. pen.,* 2011, f. 10, pag. 3638 ss.; G. DI CHIARA, *Note in tema di circolazione di atti investigativi e probatori tra procedimenti diversi,* in *Foro it.,* 1992, f. 2, p. 77 ss.; P. FELICIONI, *L'utilizzazione delle prove acquisite in altro procedimento penale: problema interpretativo o necessità di un intervento legislativo?,* in *Cass. pen*., 1992, f. 2, p. 965 ss.; L. FILIPPI, sub *art. 270,* in *Codice di procedura penale commentato*, V ed., cit., p. 2571 s.; A. NAPPI, *Sull'utilizzazione extrapenale dei risultati delle intercettazioni,* in *Cass. pen.,* 2014, f. 1, p. 386 ss.; F. RUGGIERI, *Divieti probatori e inutilizzabilità nella disciplina delle intercettazioni telefoniche*, Giuffrè, 2001, p. 102 ss. Con precipuo riguardo ai divieti di utilizzo *post* riforme, A. GASPARRE, *Condannato a causa delle intercettazioni autorizzate per reati e soggetti diversi: quelle conversazioni erano utilizzabili?,* in *Dir. e giust.,* 2019, f. 49, p. 8 ss.; L. GIORDANO, *Divieto di utilizzazione delle intercettazioni in procedimenti diversi: il rilievo dell'unitarietà iniziale*, in *Il Penalista*, 22 maggio 2019; . GALANTINI, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina*, in AA. VV., *L'intercettazione di comunicazioni*, cit. p. 227 ss.; L. PIRAS, *Utilizzabilità delle intercettazioni acquisite in altri procedimenti: precisazioni della Corte*, in *Dir. e giust*., 2018, f. 62, p. 4 ss.; P. SPERANZONI, *Quale sorte per le intercettazioni provanti ipotesi di reato diverse da quelle per le quali erano state autorizzate? Nota a ordinanza Cass. pen. sez. V, n. 11160 del 13.3.2019 (ud. 13.2.2019)*, in *Il Foro Malatestiano*, 2019, p. 1. Con riguardo all'utilizzabilità dei risultati ottenuti mediante l'impiego del *Trojan*, F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, in *Sist. pen*., 2020, f. 5, p. 233 ss.; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 257 ss.; L. GIORDANO, *La disciplina del "captatore informatico"*, in AA. VV., *L'intercettazione di comunicazioni*, cit., p. 271 ss.; W. NOCERINO, *Il captatore informatico: un giano bifronte. Prassi operative* vs *risvolti giuridici*, in *Cass. pen.,* 2020, f. 2, p. 826 ss.; G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., p. 143 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 102 ss.

[138] Cfr. nt. 136.

[139] Per dovere di completezza, si precisa che il *novum* legislativo suscita numerosi dubbi e perplessità in dottrina. Più nel dettaglio, sono astrattamente plausibili due interpretazioni dell'*explicit* dell'art. 270, comma 1 c.p.p., a seconda del significato che si voglia attribuire alla congiunzione ("e") che separa il riferimento ai delitti *ex* art.380 c.p.p. dalla menzione dell'art. 266, comma 1 c.p.p. Secondo una prima impostazione, la locuzione *de qua* avrebbe valore condizionale, nel senso che la pendenza di un diverso procedimento finalizzato all'accertamento di un delitto per cui è previsto l'arresto obbligatorio in flagranza avrebbe rilievo, ai fini dell'art. 270, comma 1 c.p.p., solo nel caso in cui tale fattispecie integrasse, al contempo, una delle ipotesi di cui all'art. 266 comma 1 c.p.p.: il reato, in sostanza, dovrebbe essere ricompreso sia nel catalogo di cui all'art. 380 c.p.p. sia in quello di cui all'art. 266 c.p.p. Secondo una differente impostazione, sarebbe più logico assegnare alla congiunzione "e" inclusa nella seconda parte dell'art. 270, comma 1 c.p.p. un valore disgiuntivo (e = oppure), sicché le conoscenze ottenute grazie all'intercettazione potrebbero essere utilizzate in un procedimento diverso in due ipotesi, tra loro del tutto equivalenti. Per una ricostruzione

nei limiti di ammissibilità previsti dalla legge[140].

In altri termini, secondo le Sezioni Unite "Cavallo" se si tratta di reati connessi *ex* art. 12 c.p.p., gli stessi non possono considerarsi "diversi" e, di conseguenza, è sempre consentita l'utilizzabilità dei risultati che emergano durante le operazioni di captazione, purché anch'essi rientrino nei limiti generali di ammissibilità di cui all'art. 266 c.p.p.; se, viceversa, si tratta di reati non connessi, valgono i limiti di cui all'art. 270 c.p.p.

Dunque, il Supremo Consesso, avallando un'interpretazione maggiormente rigorosa della disposizione[141], circoscrive la deroga al divieto di impiego extraprocedimentale dei risultati captativi alle sole ipotesi "eccezionali" al fine di evitare un indebito uso delle informazioni acquisite.

---

approfondita del dibattito de qua, K. NATALI, *Sezioni Unite e "Legge Bonafede": nuove regole per l'uso trasversale delle intercettazioni*, cit., p. 1893 ss.

[140] A tale regola fanno peraltro eccezione, come indicato dalle Sezioni Unite "Floris", le intercettazioni che costituiscano "corpo del reato" (art. 271, comma 3 c.p.p.), ossia quelle comunicazioni o conversazioni che contengano elementi di natura dichiarativa costituenti di per sé illecito penale e che integrino ed esauriscano la fattispecie criminosa (come nelle ipotesi, ad es., in cui nel corso di una telefonata si consumi una rivelazione di segreto d'ufficio o un favoreggiamento personale oppure una simulazione di reato o una minaccia), e che non si riferiscano invece meramente a una condotta criminosa o ne integrino solo un frammento, venendo portata a compimento la commissione del reato mediante ulteriori condotte rispetto alle quali l'elemento comunicativo assuma carattere meramente descrittivo. cfr. Cass., sez. un., 26 giugno 2014, n. 32697, in *Dir. pen. proc*., 2014, f. 12, p. 1448 ss., con nota di A. INNOCENTI, *Le Sezioni Unite aprono all'utilizzabilità dei risultati di intercettazioni disposte in "diverso procedimento*".

[141] In particolare, un primo orientamento esclude che nella nozione di procedimento diverso vi rientrino i procedimenti che abbiano ad oggetto indagini strettamente connesse o collegate sotto il profilo oggettivo, probatorio e finalistico al reato in relazione al quale le operazioni di intercettazioni sono state disposte. Cfr. Cass., sez. III, 28 febbraio 2018, n. 28516, in *CED. Cass*., n. 273226; sez. V, 20 gennaio 2015, n. 26693, i*vi*, n. 264001; sez. III, 23 settembre 2014, n. 52503, *ivi,* n. 261971; sez. II, 10 ottobre 2013, n. 3253, *ivi,* n. 258591; sez. II, 11 dicembre 2012, n. 49930, *ivi,* n. 253916; sez. VI, 15 novembre 2012, n. 46244, *ivi*, n. 254285; sez. VI, 10 maggio 1994, n. 2135, *ivi,* n. 199917. Un secondo orientamento, di formazione più recente ma che negli ultimi anni si è fatto strada con una certa determinazione, ritiene invece che, una volta che siano state legittimamente disposte le intercettazioni per un determinato titolo di reato riconducibile al catalogo di cui all'art. 266 c.p.p., le risultanze probatorie emerse dalle predette operazioni siano utilizzabili per tutti i reati relativi al medesimo procedimento, posto che la disciplina dell'art. 270 c.p.p. entra in gioco soltanto in caso di procedimento originariamente diverso mentre non si applica all'ipotesi di procedimento successivamente frazionato a causa della eterogeneità delle ipotesi di reato e dei soggetti indagati. In tal senso si vedano Cass., sez. V, 9 febbraio 2018, n. 15288, in *C.E.D.,* n. 272852; sez. VI, 26 aprile 2017, n. 31984, *ivi,* n. 270431; sez. VI, 1 marzo 2016, n. 21740, *ivi,* n. 266921; sez. II, 23 febbraio 2016, n. 9500, *ivi,* n. 267784; sez. VI, 25 novembre 2015, n. 50261, *ivi,* n. 265757; sez. VI, 15 luglio 2015, n. 41317, *ivi,* n. 265004; sez. IV, 8 aprile 2015, n. 29907, *ivi*, n. 264382; sez. VI, 16 dicembre 2014, n. 6702, *ivi*, n. 262496; sez. VI, 4 novembre 2014, n. 53418, *ivi,* n. 261838. Un terzo e risalente indirizzo escludeva invece, al di fuori dei casi tassativamente indicati dall'art. 270 c.p.p., la possibilità di utilizzazione delle risultanze captative in diverso procedimento anche in ipotesi di connessione oggettiva o probatoria. Si vedano Cass., sez. III, 3 luglio 1991, n. 9993, in *C.E.D. Cass.,* n. 188356; sez. IV, 11 dicembre 2008, n. 4169, *ivi,* n. 242836 e, più di recente, sez. II, 11 dicembre 2012, n. 49930, *ivi,* n. 253916. Tra i diversi orientamenti esistenti, le Sezioni Unite hanno invero optato per una quarta interpretazione, che valorizza il più restrittivo «criterio di valutazione sostanzialistico» incentrato solo sulla connessione *ex* art. 12 c.p.p. *stricto sensu* intesa e non più sul mero collegamento investigativo e men che meno sulla unitarietà iniziale del procedimento. In questo senso G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità,* cit., p. 144.

Ecco, quindi, la ragione per cui la scelta del legislatore appare quanto mai stravagante, operando un *renvirement* inaspettato e ingiustificato rispetto ai più ragionevoli approdi giurisprudenziali[142], improntati al raggiungimento di un equilibrio tra esigenze investigative e tutela delle prerogative individuali, nel pieno rispetto della garanzia costituzionale della motivazione del decreto autorizzativo[143].

Più precisamente, attraverso la modifica del comma 1 dell'art. 270 c.p.p., l'ultimo legislatore – oltrepassando il monito delle Sezioni Unite "Cavallo" – amplia a dismisura il perimetro di operatività dell'utilizzabilità dei dati captati in procedimenti diversi che, *de facto*, risulta essere consentita anche per l'accertamento di tutte le fattispecie ricomprese nell'ambito dell'art. 266, comma 1 c.p.p., ossia per l'enorme e variegato catalogo dei reati suscettibili di intercettazione, a cui si aggiunge la nuova fattispecie dei «delitti commessi avvalendosi delle condizioni previste dall'articolo 416 *bis* c.p. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo»[144].

Inoltre, ai sensi del riformato comma 1 *bis* della medesima disposizione, fermo restando il divieto di impiego del prodotto delle captazioni in procedimenti diversi da quelli nei quali le stesse sono state disposte[145], «[…] i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile possono essere utilizzati anche per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, se compresi tra quelli indicati dall'articolo 266, comma 2 *bis*» c.p.p.[146], condizionando il loro impiego al canone della «indispensabilità»[147].

Allo stato, dunque, è possibile utilizzare le risultanze delle attività captative condotte mediante

---

[142] A questo proposito non possono trascurarsi le pronunce della Suprema corte che, prima della decisione delle Sezioni Unite "Cavallo", avevano introdotto un "correttivo" all'impiego processuale dei dati acquisiti in diversi procedimenti. In particolare, si è affermato che nel caso di utilizzo in un diverso procedimento di intercettazioni compiute *aliunde*, dinanzi alle eccezioni formulate dall'imputato o dall'indagato, il giudice è tenuto ad effettuare in via incidentale il controllo sulla legittimità delle captazioni. Cass., sez. II, 26 aprile 2012, n. 30815, in *C.E.D. Cass*., n. 253415. Più di recente, sez. VI, 13 giugno 2017, n. 36874, *ivi*, n. 270812. Con precipuo riferimento alla circolazione dei dati acquisiti tramite *Trojan*, sez. VI, 13 giugno 2017, n. 36874, in *Dir. pen. cont.*, 27 settembre 2017.

[143] Secondo Corte cost., 11 luglio 1991, n. 366, l'utilizzazione delle intercettazioni come prova in altro procedimento trasformerebbe l'intervento del giudice richiesto dall'art. 15 Cost., vanificando l'esigenza più volte affermata dal giudice delle leggi che il provvedimento giudiziale sia puntualmente motivato, in una inammissibile "autorizzazione in bianco", con conseguente lesione della sfera privata legata alla garanzia della libertà di comunicazione e al connesso diritto di riservatezza incombente su tutti coloro che ne siano venuti a conoscenza per motivi di ufficio. Secondo la Corte dunque la disciplina dettata dall'art. 270 c.p.p. individua un ragionevole punto di equilibrio tra primarie esigenze di tutela dell'individuo, inerenti al nucleo dei diritti fondamentali, e l'interesse pubblico primario all'accertamento dei reati, equilibrio incentrato sull'intervento del giudice, cui spetta di dar conto degli specifici presupposti per autorizzare l'attività captativa, da ritenersi strettamente correlato all'ambito di quella autorizzazione, con la conseguenza che l'utilizzabilità degli esiti non può non dipendere da quella correlazione, in rapporto alla concreta disciplina dettata dal legislatore.

[144] Ai sensi dell'art. 266, comma 1, lett. *f quinquies,* c.p.p. Come precisato, «[L]la nuova ipotesi di intercettazione si aggiunge alla già lunghissima lista dei delitti suscettibili di intercettazione e può riguardare anche reati bagatellari ma aggravati da tale modalità "mafiosa" con una pena che non avrebbe consentito *ex se* l'intercettazione». Così L. FILIPPI, *Intercettazioni:* habemus legem!, cit., p. 454.

[145] *Ex* art. 270, comma 1, c.p.p.

[146] Cfr. art. 2, comma 1, lett. *g)*, punto 1, d.l. n. 161/2019.

[147] L. n. 7/2020, che modifica l'art. 2, comma 1, lett. *g)*, d.l. n. 161/2019.

Trojan non solo in procedimenti diversi per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza e di quelli di cui all'art. 266, comma 1 c.p.p., ma anche per la prova di reati diversi da quelli contemplati dal decreto autorizzativo, purchè ricompresi tra i gravi crimini di cui all'art. 51, commi 3 *bis* e 3 *quater,* c.p.p. e quelli commessi dai pubblici ufficiali o gli incaricati di pubblico servizio contro la pubblica amministrazione[148].

Anche sul punto si avanzano delle riserve, intravedendo nella modifica *de qua* l'intento del legislatore di ribaltare il rapporto tra norma ed eccezione[149]. A ben guardare, infatti, la contro-riforma tende a sgretolare la regola dell'inutilizzabilità probatoria del captato in procedimenti diversi, estendendo il perimetro di operatività del regime derogatorio. Ciò non senza conseguenze

---

[148] Come precisato, la formulazione non appare chiarissima, non risultando facilmente interpretabile il significato della clausola di apertura del comma 1 *bis*, laddove fa salvo il disposto del primo comma dell'art. 270 c.p.p. Secondo G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità,* cit., p. 146, «[N]non è chiaro, tuttavia, se con tale modifica il legislatore consapevole abbia voluto restringere il panorama applicativo dei risultati delle intercettazioni tra presenti mediante captatore informatico rispetto alle intercettazioni "classiche", superando così il *dictum* delle Sezioni Unite "Cavallo" attraverso l'enucleazione di un nuovo e diverso criterio per l'utilizzabilità di tali risultati nei confronti di reati diversi, ritenendo non più rilevante il requisito della stretta connessione sostanziale tra i reati e limitando per contro la loro utilizzabilità, oltre che ai delitti per cui sia previsto l'arresto obbligatorio in flagranza, alle sole fattispecie indicate dall'art. 266 comma 2 *bis* c.p.p., ossia ai soli delitti di cui agli artt. 51 commi 3 *bis* e 3 *quater* c.p.p. (reati di criminalità organizzata e terrorismo) e ai delitti dei pubblici ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni». Secondo F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, cit., p. 238 e 245, «[I]il riferimento al comma primo della disposizione sembra rinviare alla utilizzabilità dei risultati captativi con riguardo ai reati ad arresto obbligatorio emersi nel corso dell'attività e non anche […] ai reati connessi a quello per cui siano state autorizzate le operazioni tramite captatore né, indistintamente, ai reati contemplati dall'art. 266, comma 1, c.p.p. cui oggi il comma primo dell'art. 270 c.p.p […] rinvia […] Alla luce di tali considerazioni […] la soluzione interpretativa, costituzionalmente orientata, appare cogente, nel senso di ritenere che il richiamo al primo comma che opera l'art. 270, comma 1 *bis* c.p.p. sia limitato ai soli reati ad arresto obbligatorio, cui si aggiungono – quanto alla possibilità di una migrazione del materiale acquisito tramite *trojan*, ai fini della prova di reati diversi da quello per cui le operazioni siano state autorizzate – i reati di cui all'art. 266, comma 2 *bis* c.p.p., gli uni e gli altri configurando sottoinsiemi omogenei, quanto a gravità ed offensività, che giustificano ampiamente l'eccezionale deroga alla ordinaria immanenza dei risultati intercettativi al – solo – reato oggetto di autorizzazione, dovendo farsi applicazione, quale criterio di impiego processuale, del requisito della indispensabilità, ai fini della prova del reato diverso, del contenuto auditivo oggetto di captazione nel corso delle operazioni disposte con riguardo al reato per cui erano state autorizzate». In sede applicativa, si è detto che «[D]deve […] ritenersi la disciplina di utilizzabilità delle intercettazioni tramite captatore per i reati diversi da quelli oggetto di autorizzazione sia esaustivamente collocata nel comma 1 *bis* dell'art. 270 c.p.p., cosicchè i relativi esiti possono essere utilizzati per reati diversi solo alle condizioni *ivi* stabilite: tali esiti devono essere indispensabili per l'accertamento dei soli delitti indicati dall'art. 266, comma 2 *bis* c.p.p.». Così Linee-guida della procura della Repubblica di Bologna, *La nuova disciplina delle intercettazioni. Profili di interesse per l'Ufficio del pubblico ministero*, cit.

[149] Come sostenuto, «[I]il risultato finale, apprezzabile agevolmente alla luce della stessa *littera legis*, sembra rovesciare il rapporto tra regola ed eccezione: l'estensione dei risultati intercettativi ai procedimenti diversi […] ha tradizionalmente rappresentato una deroga all'inesportabilità di quei risultati, giustificata […] da ragioni politico-criminali – legate al disvalore ed all'offensività espressa dai reati soggetti ad arresto obbligatorio –, in grado di prevalere sul concorrente *asset* costituzionale della libertà e segretezza delle comunicazioni». Così Secondo F. ALVINO, *La circolazione delle intercettazioni e la riformulazione dell'art. 270 c.p.p.: l'incerto pendolarismo tra regola ed eccezione*, cit., p. 240.

sul piano processuale: nell'ottica di un coordinamento con l'interpretazione fornita dalla Suprema Corte al concetto di "diverso reato" e "diverso procedimento"[150], si deve ritenere che il divieto di circolazione delle informazioni apprese mediante captatore non operi (oltre che in relazione ai casi espressamente previsti dal dettato normativo di cui al comma 1 dell'art. 270 c.p.p., espressamente richiamato nell'*incipit* del comma 1 *bis* del medesimo articolo), con riferimento ai reati diversi ma connessi *ex* art. 12 c.p.p.[151], nonché ai reati diversi non connessi che rientrano nei casi di cui all'art. 266, comma 2 *bis* c.p.p.[152].

La novella apre, dunque, la strada "libera" circolazione probatoria delle risultanze della captazione digitale determinando una sostanziale violazione della garanzia della riserva di giurisdizione prevista dall'art. 15 Cost.[153], con riferimento all'intercettazione confluita nel "procedimento diverso", in assenza di qualsivoglia controllo da parte del giudice procedente.

Il rischio è che una volta ottenuta l'autorizzazione all'impiego del *virus* informatico in riferimento ad un certo reato all'interno di un determinato procedimento – e quindi anche sulla base di motivi concernenti la posizione dell'indagato in quel procedimento per quella specifica fattispecie delittuosa – le informazioni ottenute possano essere utilizzate anche in indagini diverse per la prova di reati differenti, benché, in questi non sussistano o comunque non siano stati verificati i presupposti per l'emissione di un analogo provvedimento autorizzativo[154].

Il tutto aggravato dal carattere itinerante tipico del *malware*, in grado di "seguire" ogni spostamento del sorvegliato senza limiti di tempo e spazio e, di conseguenza, acquisire una mole di dati assai più cospicua rispetto a quella ottenibile mediante gli strumenti tradizionali di captazione, anche con riferimento a soggetti terzi estranei all'indagine. Pericolo che si fa particolarmente acuto nei casi in cui l'attività di controllo venga effettuata in procedimenti per i reati distrettuali ed economici, in relazione ai quali nessuna specifica cautela è stabilita a salvaguardia del domicilio privato.

Da ultimo, non rimane che soffermarsi sulla modifica operata all'art. 271 c.p.p. già nel 2017 e confermata dalle successive legislature.

Come noto, secondo il *dictum* di cui all'art. 271, comma 1 *bis* c.p.p., «[N]non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore

---

[150] Secondo Cass., sez. un., 28 novembre 2019, n. 51, cit., il concetto di procedimento diverso non si identifica con la nozione di reato diverso. Come sostenuto, tuttavia, «[L]la contrapposizione tra reato e procedimento, richiamata anche dalla sentenza in esame, non trova in realtà riscontro nel lessico del codice […]. Che si parli di reati o di procedimenti, dunque, l'unica cosa che dovrebbe rilevare è che dalle intercettazioni sia emerso un fatto nuovo, non contemplato in precedenza». G. ILLUMINATI, *Utilizzazione delle intercettazioni in procedimenti diversi: le sezioni unite ristabiliscono la legalità costituzionale*, cit.

[151] Per cui, è bene precisarlo nuovamente, non opera il divieto di cui all'art. 270, comma 1, c.p.p., non trattandosi di "reati diversi". Cfr. Cass., Sez. un., 28 novembre 2019, n. 51, cit.

[152] Sul punto, efficacemente, G. PESTELLI, *La controriforma delle intercettazioni di cui al d.l. 30 dicembre 2019 n. 161: una nuova occasione persa, tra discutibili modifiche, timide innovazioni e persistenti dubbi di costituzionalità*, cit., 147. Cfr. Delibera CSM, *Parere sul disegno di legge 1659 AS di conversione del d.l. 161/2019*, cit., p. 5.

[153] Sul punto, esaustivamente, A. CAMON, *Le intercettazioni telefoniche nel processo penale*, cit., p. 44. Più di recente e con riferimento alla normativa modificata nel 2017, P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 255 ss.

[154] P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 262; ID., *L'impiego del* trojan horse *informatico nelle indagini penali*, cit., p. 329 ss. Un simile rischio è, inoltre, paventato da R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 538 ss.

informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo».

Prima facie, l'innesto *de qua* potrebbero sembrare lodevole in quanto finalizzato a limitare i danni derivanti da uno strumento che *ex se* riesce ad apprendere più di quanto richiesto; eppure, a ben guardare, il *novum* non risulta così rassicurante come sembra.

Intanto, l'inutilizzabilità colpisce «l'idoneità della prova a produrre risultati conoscitivi valutabili dal giudice per la formazione del suo libero convincimento»[155], di conseguenza, i risultati inutilizzabili a fini probatori non perderanno valore a fini investigativi, potendo comunque essere utilizzati dagli inquirenti come "spunti" per l'avvio di ulteriori indagini[156].

Ecco, quindi, il paradosso. Pur non potendo formalmente utilizzare i risultati intercettivi ottenuti mediante le captazioni a mezzo di *virus* informatico per formare il convincimento del giudice, gli stessi possono essere impiegati dagli inquirenti per stimolare la formazione di una nuova *notitia criminis*, potendo, sulla base degli stessi, avviare le necessarie investigazioni funzionali all'inizio di un procedimento penale[157].

In sostanza, sulla base delle informazioni acquisite, la polizia giudiziaria potrà compiere tutti quegli atti "atipici" di indagine[158] per i quali non è prevista una «possibile partecipazione del difensore al compimento dell'atto»[159] ed il pubblico ministero potrà utilizzare «gli strumenti più appropriati, modellati sulla struttura degli atti di indagine che vengono compiuti durante le attività amministrative o procedimentali»[160].

Non solo. Il divieto di utilizzo obliquo dei risultati ottenuti *ultra* e *contra legem* riguarda solo il contenuto delle conversazioni e delle comunicazioni apprese mediante il *Trojan*, non estendendosi, per converso, a quel complesso di operazioni che pur possono essere esperite tramite il captato.

---

[155] Così A. CHELO, *Intercettazioni telefoniche e divieto di utilizzabilità: quale significato alla nozione di diverso procedimento?*, cit., p. 1422.

[156] Simili rilievi appartengono anche a L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, in AA. VV., *Nuove norme in tema di intercettazioni*, cit., p. 290; EAD., voce *Perquisizioni* on line, in *Enc. dir.*, Annali, X, Giuffrè, 2017, p. 619 s.; M. TROGU, *Intrusioni segrete nel domicilio informatico*, in AA. VV., *Le indagini atipiche*, II ed., cit., p. 583 s.

[157] Tale ragionamento ben può essere esteso nell'ipotesi di inutilizzabilità prevista *ex* art. 270, comma 1 *bis* c.p.p. Infatti, nulla esclude che i risultati intercettivi possano valere come nuova notizia di reato, come punto di partenza per le nuove indagini e per l'acquisizione di ulteriori spendibili fonti di prova. Di questo avviso, da ultimo, Cass., sez. VI, 22 aprile 2016, n. 34450, in *Dir. pen. proc.,* 2017, n. 12, p. 1607 ss., con nota di W. NOCERINO, *Le denunce anonime come strumento di indagine. Un difficile equilibrio tra efficienza e garanzie.* Una simile possibilità è prevista sotto un profilo operativo. Cfr. Linee-guida della procura della Repubblica di Bologna, *La nuova disciplina delle intercettazioni. Profili di interesse per l'Ufficio del pubblico ministero*, cit. Più in generale, sul tema della pre-inchiesta si rinvia a R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, Jovene, 2010, p. 60 ss.; A. MARANDOLA, *I registri del pubblico ministero*, Cedam, 2001, p. 70 ss.; A. ZAPPULLA, *La formazione della notizia di reato*, Giappichelli, 2012, p. 248 ss. Si consenta, inoltre, un rinvio a W. NOCERINO, *Le intercettazioni e i controlli preventivi sulle comunicazioni. Riflessi sul procedimento probatorio*, Wolters Kluwer-Cedam, 2019, p. 169 ss.

[158] Quali, ad esempio, pedinamenti, identificazioni, rilievi segnaletici, descrittivi o fotografici. Sul tema, per tutti, C. FANUELE, *La ricostruzione del fatto nelle investigazioni penali,* Cedam, 2012, p. 31 s.

[159] Così, FANUELE, *L'utilizzazione delle denunce anonime per l'acquisizione della notizia di reato: condizioni e limiti delle attività pre-procedimentali alla luce delle regole sul "giusto processo*", in *Cass. pen.*, 2012, f. 4, p. 1555.

[160] L'espressione appartiene a R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 52.

Di conseguenza, il divieto di cui all'art. 271, comma 1 *bis* c.p.p., rimane del tutto formale, dal momento che i dati diversamente appresi potrebbero trovare ingresso nel processo penale attraverso i "tradizionali" canali di acquisizione delle prove atipiche[161].

8. La fallace disciplina della conservazione del captato. La catena di custodia e la distruzione del *virus*

In relazione ai profili che regolano le attività subentranti alla captazione *strictu sensu* intesa, l'art. 89 disp. att. c.p.p. viene arricchito di una serie di commi deputati a regolamentare il contenuto del verbale delle operazioni di p.g., i programmi da utilizzare nonché le cautele da rispettare al fine di garantire l'integrità della catena di custodia[162].

La normativa avanguardistica delineata sin dalle prime riforme, appare nel suo complesso apprezzabile, denotando l'interesse del legislatore a confrontarsi con degli aspetti più propriamente "tecnici", concernenti il "tracciamento" delle operazioni compiute, ossia il complesso di attività da svolgere al fine di garantire l'«originalità»[163] e l'«integrità» delle registrazioni[164], conformemente ai *dicta* provenienti dalla l. 18 marzo 2008, n. 48[165].

---

[161] Sul tema, esaustivamente, AA. VV., *Le indagini atipiche*, II ed., cit., *passim*.

[162] *Ex* art. 5, d.lgs. n. 216/2017. La catena di custodia può essere definita come «quell'insieme di passaggi, formalizzati con un sistema di tracciamento, attraverso cui [il dato] transita (correttamente) […] al giudizio». Così, R. GENNARI-L. SARAVO, *Le tracce*, in AA. VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche e scienza*, a cura di D. Curtotti-L. Saravo, Giappichelli, 2019, p. 446 s. Per una panoramica della regolamentazione "tecnica" delle intercettazioni tramite captatore informativo, Così S. ATERNO, *Il punto di vista degli operatori. Il difensore*; cit., p. 333 s.; T. BENE, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, in *Arch. pen.,* 2019, f. 3, p. 9 ss.

[163] La perfetta corrispondenza all'originale è consentita soltanto dalla *bitstream image*; a tal fine si richiede che il supporto sia vergine. Per approfondimenti, S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc.,* 2008, f. 6, *Dossier* su *La prova scientifica nel processo penale,* a cura di P. Tonini.

[164] L'integrità dei dati acquisiti è garantita tramite l'algoritmo di *hash*, che consente di creare, attraverso una funzione matematica, una sequenza di *bit* di lunghezza variabile. In giurisprudenza, da ultimo, Cass., sez. III, 28 maggio 2015, in *C.E.D. Cass.,* n. 265180. Sul tema *de qua*, esaustivamente, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 122 ss. Come di recente precisato dalla Suprema corte, una simile procedura non deve essere impiegata ogni volta in cui ci si trova difronte a documenti informatici. Così, «[L]l'utilizzabilità delle videoriprese eseguite da privati con telecamere di sicurezza non è subordinata alla procedura di estrazione dei dati archiviati in un supporto informatico prevista dall'art. 254 *bis* c.p.p., la cui inosservanza non è assistita da alcuna sanzione processuale, potendone derivare, invece, eventualmente, effetti sull'attendibilità della prova». Cass., sez. VI, 6 maggio 2020, n. 13779, in *Proc. pen. giust*., 6 maggio 2020.

[165] L. 18 marzo 2008, n. 48, recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*", in *Gazz. uff*. 4 aprile 2008, n. 80. Per un quadro di insieme della l. 48 del 2008, L. CORDÍ, sub *art. 8 l. 18.3.2008, n. 43,* in *Legislaz. pen*., 2008, p. 282 ss.; R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen. cont*., 20 settembre 2012; G. RESTA, *La disciplina acquista maggiore organicità per rispondere alle esigenze applicative*, in *Guida dir*., 2008, f. 16, p. 52 ss.; ID., Cybercrime *e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 2008, p. 2147 ss.; P. SCOGNAMIGLIO, *Criminalità informatica*. *Commento organico alla Legge 18 marzo 2008, n. 48*, Edizioni Giuridiche Simone, 2008. Sui profili processuali, S. ATERNO, *Modifiche al titolo III del libro*

Più nel dettaglio, la scelta di "rinvigorire" il contenuto del verbale redatto dalla p.g. al fine di documentare l'attività svolta, risulta assolutamente condivisibile: lo stesso non solo deve recare una dettagliata esposizione del personale coinvolto, dell'ora di inizio e fine delle operazioni, dei luoghi e dei tempi oggetto di captazione ma anche attestare tutto quanto avviene dopo la disinstallazione del *virus* dal dispositivo in cui era stato inoculato[166], in modo da tracciare l'intero *iter* seguito dalla stessa nel trasferimento delle registrazioni. Ciò nell'ottica di consentire sia all'autorità giudiziaria che alle altre parti processuali di verificare la correttezza dei singoli passaggi eseguiti. Altrettanto pregevole appare la volontà delineare un modello di captatore "legale" attraverso la predisposizione di una griglia di requisiti che il programma spia deve soddisfare per essere considerato tale: ai fini dell'istallazione e dell'intercettazione a mezzo *Trojan*, infatti, devono essere impiegati soltanto programmi conformi ai requisiti tecnici stabiliti con decreto del Ministero della giustizia[167]. Ancora, è assolutamente condivisibile è la scelta di trasferire il captato esclusivamente verso gli impianti della procura della Repubblica, al fine di impedire la c.d. remotizzazione della registrazione, assai diffusa nella prassi, e che, peraltro, secondo un discutibile indirizzo giurisprudenziale consolidato, non inciderebbe sulla genuinità del dato registrato[168].

A prescindere dallo sforzo disciplinare effettuato nel 2017 e ritoccato nel corso degli anni, non possono sottacersi alcune sviste del frettoloso legislatore.

In primis, si avanzano delle perplessità in relazione al *dictum* che prevede la conformità del captatore informatico in uso alla p.g. ai requisiti tecnici previsti dal decreto ministeriale.

In effetti, un decreto ministeriale è già stato emanato[169] e ha trovato un'«attuazione deludente»[170]: disattendendo le aspettative dei tecnici che reclamavano la predisposizione di regole più rigorose in relazione al funzionamento del captatore informatico anche in rapporto al costante progresso tecnologico[171], l'art. 4 del d.m. 20 aprile 2018 si limita ad indicare i requisiti

---

terzo del codice di procedura penale, in AA.VV., Cybercrime, *responsabilità degli enti, prova digitale*. *Commento alla Legge 18 marzo 2008, n. 48*, a cura di G. Corasanti-G. Corrias Lucente, Cedam, 2009, p. 193 ss.; M.L. DI BITONTO, *L'accertamento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 2008, p. 503 ss.; L. LUPARIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I profili processuali*, in *Dir. pen. proc.*, 2008, f. 7, p. 717 ss.; N. VENTURA, *Ratifica della Convenzione di Budapest e iniziativa investigativa della polizia giudiziaria*, in *Giust. pen.,* 2008, f. 1, p. 225 ss.; F.M. MOLINARI, *Le attività investigative inerenti alla prova di natura digitale*, in *Cass. pen.,* 2013, f. 12, p. 1259 ss. Più di recente, S. ATERNO, *La convenzione di Budapest del 2001 e la L. n. 48/2008*, in AA. VV., Cybercrime. *Trattato di diritto penale*, a cura di A. Cadoppi-S. Canestrari-A. Manna-M. Papa, Utet, 2019, p. 1351 ss.; M. DANIELE, *Intercettazioni ed indagini informatiche*, in AA. VV., *Manuale di procedura penale europea*, a cura di R. E. Kostoris, 2017, p. 433 ss.

[166] Imponendo l'immediata distruzione del *virus.* Cfr. P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 131 ss.

[167] Alla "possibilità" inizialmente prevista dal d.l. n. 216/2017, si contrappone il "dovere" imposto dalla novella del 2020.Cfr. l. n. 7/2020, che modifica l'art. 2, comma 2, lett. *a)*, d.l. n. 161/2019.

[168] Sulla legittimità della prassi della cd. remotizzazione, si veda Cass., sez. un., 26 giugno 2008, n. 36359, in *C.E.D. Cass.,* n. 240395. L'orientamento è pressochè costante. Cfr. sez. VI, 17 novembre 2015, n. 47504, in *Cass. pen.,* 2016, f. 6, p. 2572; sez. I, 21 ottobre 2015, n. 49918, inedita; sez. IV, 27 novembre 2014, n. 5401, in *C.E.D. Cass.,* n. 262126; sez. VI, 4 novembre 2014, n. 53418, *ivi*, n. 261838; sez. III, 7 gennaio 2014, n. 1116, *ivi,* n. 259744.

[169] D.m. 20 aprile 2018, recante "*Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7, commi 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216*", Bollettino ufficiale del Ministero della Giustizia, 31 maggio 2018, n. 10.

[170] Così T. BENE, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, cit., p. 6.

[171] Lo stesso, infatti, avrebbe dovuto tenere costantemente conto dell'evoluzione tecnica al fine di garantire che tali programmi si limitassero ad effettuare le operazioni espressamente disposte

che allo stato i programmi devono contenere per essere considerati legali. In questo modo, si profila rischio – assai concreto – di «precoce obsolescenza [del decreto stesso], con la conseguenza che si mostra necessario un tempestivo e continuo aggiornamento delle regole, onde evitare uno svuotamento di tutela»[172].

Non solo. Si tratta di un regolamento tecnico «non sufficientemente puntuale»[173] nello specificare il monitoraggio e il tracciamento continuo (c.d. *logging*) di tutta l'attività che svolge il *client* attaccante sul computer: se il pericolo da scongiurare è quello di evitare che il trasferimento dei dati possa determinarne una diffusione, è altrettanto palese che il legislatore sia stato superficiale nel non introdurre regole precise atte di evitare "fughe di notizie". Se l'*hashing* ormai viene effettuato di *default* dai *software* di ultima generazione su tutti i *files* esfiltrati, in relazione agli usi più avanguardistici del *virus*, sarebbero indispensabili regole più rigide e stringenti quali l'apposizione di firme digitali e di marcature temporali sia ai *log* di registro sia ai *files* prodotti dal sistema, nonché a quelli relativi all'acquisizione[174].

Il tutto aggravato dal fatto che molto spesso, nella prassi, le attività di intercettazione mediante *virus* informatico sono appaltate a società esterne private autorizzate dall'autorità giudiziaria a svolgere le intercettazioni[175]. Come dimostrano le più recenti vicende giudiziarie[176], il rischio

---

secondo *standard* idonei di affidabilità tecnica, di sicurezza e di efficacia. L'idea sottesa sembra diretta a scongiurare il rischio di utilizzare *software* più evoluti, capaci di compiere attività più penetranti, come, per esempio, la perquisizione a distanza del dispositivo bersaglio.

[172] Così M. TORRE, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, cit., p. 147.

[173] Cfr. S. Aterno, *Appunti riassuntivi dell'audizione presso la Commissione giustizia del Senato della Repubblica in relazione alla conversione in legge del d.l. 30 dicembre 2019, n. 161 e, in particolare, per la materia delle intercettazioni per la materia delle intercettazioni attraverso sistemi di captazione informatica*, cit., p. 3.

[174] S. ATERNO, *Il punto di vista degli operatori. Il difensore*, p. 322, per cui «[G]garantire la verificabilità *ex post* dei *files* acquisiti dal captatore nel momento in cui vengono acquisiti dall'intero sistema […] e la conseguente sicurezza che non è stato possibile per nessuno manipolarli, rappresenta la garanzia minima che si possa pretendere da una legge tanto invasiva per i diritti e le libertà individuali».

[175] In conformità al disposto di cui all'art. 268, comma 3 *bis* c.p.p., in forza del quale «per le operazioni di avvio e di cessazione delle registrazioni, mediante inserimento di captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, comma 4» c.p.p. D'altra parte, si ritiene si ritiene sul punto che sia irrilevante, ai fini del rispetto del disposto di cui all'art. 268 c.p.p., che le operazioni si svolgano in procura con strumentazione appartenente a privati. Si veda Cass. 19 dicembre 2014, n. 3137, in *C.E.D. Cass*., n. 262485. Non solo. La giurisprudenza si spinge fino a prevedere che l'impiego di ausiliari tecnici, come gestori dei sistemi informatici utilizzati, «è assolutamente necessario per realizzare l'attività investigativa». Così Cass., sez. III, 10 novembre 2015, n. 50452, in *Cass. pen*., 2016, f. 7-8, p. 2941; sez. III, 5 marzo 2009, n. 16683, inedita. Di recente, sez. VI, 27 novembre 2018, n. 14395, in *C.E.D. Cass.,* n. 275534. Per un commento v. L. GIORDANO, Blackberry Messenger: *l'indisponibilità dell'algoritmo per decriptare i dati informatici non lede il diritto di difesa,* in *Il Penalista,* 28 aprile 2019. La *questio de qua* è approfondita da T. BENE, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, cit., p. 9 ss.; D. PRETTI, *La metamorfosi delle intercettazioni: la contro-riforma Bonafede e l'inarrestabile mito della segretezza delle comunicazioni,* cit., p. 102 ss.; A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite virus informatico*, cit., p. 607; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 181.

[176] Ci si riferisce al caso Exodus. Essa coinvolge una società sviluppatrice di piattaforme informatiche e di *software* per lo svolgimento di intercettazioni telematiche mediante captatore informatico. Tra le piattaforme anche *Exodus*, utilizzata, per le intercettazioni tramite *Trojan*, da aziende, divenute ausiliari della polizia giudiziaria. L'indagine dovrà accertare le caratteristiche di funzionamento della

derivante dalla partecipazione di soggetti estranei alla polizia giudiziaria nell'attività di indagine, è legato all'impossibilità di garantire la segretezza dell'attività investigativa, impedendo ogni forma di abuso delle società appaltatrici[177], dal momento che in questo settore manca una disciplina inerente alle modalità di acquisizione delle tecnologie rivolte e destinate alla captazione di comunicazioni[178] e, più in generale, risultano totalmente assenti linee guida ministeriali, dirette a regolamentare i rapporti con le società di intercettazione.

Per tali ragioni, sarebbe urgente una modifica del decreto ministeriale che, nell'ottica di un coordinamento con la disciplina modificata, determini con la massima chiarezza i requisiti tecnici e le coordinate spazio-temporali dell'intercettazione tramite captatore.

Infine, con riferimento alla procedura di distruzione del captatore informatico, la disinstallazione degli stessi dalla macchina bersaglio porrebbe non pochi problemi di ordine pratico: dovendo questa avvenire necessariamente da remoto, potrebbero perdersi le tracce e il controllo stesso del *virus*, banalmente perché il dispositivo elettronico non si connette più alla rete, permettendo, dunque, un monitoraggio "perenne" dello stesso, che travalica le finalità per cui viene autorizzato.

Si creerebbero, così, problemi anche in tema di *data retention*: la conservazione dei dati personali, come di recente precisato dalla Corte di giustizia, può avvenire «solo nel rispetto del principio di proporzionalità, nel bilanciamento tra diritto alla protezione dei dati personali ed

---

piattaforma informatica e le modalità con cui i dispositivi degli utenti venivano infettati, dopo aver scaricato una particolare *app*. Il sospetto è che sia stato effettuato un numero infinito di intercettazioni non autorizzate dall'autorità giudiziaria, tramite un virus utilizzato dalle società, i cui dati sarebbero stati conservati in spazi *cloud* della piattaforma Amazon, con sede negli Stati Uniti. La gravità dell'operazione sembra non arrestarsi, almeno fino a quando non verranno individuati i limiti del contratto di sperimentazione che i servizi segreti italiani avevano stipulato nel 2016 con la stessa società che gestiva Exodus. Cfr. Cass., sez. VI, 26 aprile 2019, n. 31579, in *www.forensicsgroup.eu.* Per commenti, S. ATERNO-F. PIETROSANTI*, Intercettazioni via* trojan, *come evitare un nuovo caso* Exodus: *i problemi da risolvere*, 9 Aprile 2019, in *www.agendadigitale.eu*; F. BRIZZI, *Il captatore informatico: un* Exodus *verso "buone pratiche"?,* in *Il Penalista*, 4 settembre 2019.

[177] Come precisato da A. SANNA, *L'irriducibile atipicità delle intercettazioni tramite virus informatico*, cit., p. 607, «il nodo di fondo è rappresentato dal momento esecutivo delle operazioni, sottratto, per un insieme di fattori, al controllo dell'autorità inquirente». Ciò non solo per la dislocazione fisica delle società private dalla centrale di controllo ma anche e soprattutto per ragioni di natura tecnica. I programmi impiegati per le finalità investigative, sviluppati da aziende specializzate, sono "*proprietar*", occultano, cioè, i loro codici sorgente, per cui risulta impossibile controllare le modalità di funzionamento e il grado di affidabilità e sicurezza dei risultati. Secondo F. BRIZZI, *Il captatore informatico: un* Exodus *verso "buone pratiche"?,* cit., «[l]il ricorso a tali due tipologie di sistemi (*app* o comunque *software* che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a tutti e, per altro verso, archiviazione mediante sistemi *cloud* in *server* posti fuori dal territorio nazionale) dovrebbe, dunque, essere oggetto di un apposito divieto». Secondo altra parte della dottrina, sarebbe sufficiente dotare il *software* di un adeguato sistema di *logging* di tutte le azioni svolte dal dispositivo, sì da registrare ogni operazione di accesso ai dati, al sistema, alle periferiche (R. BRIGHI, *Funzionamento e potenzialità investigative del* malware, in AA. VV., *Nuove norme in tema di intercettazione. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, cit., p. 231), oppure a meccanismi di *report* delle attività compiute (M. TORRE, il *captatore informatico, tra riforma Orlando e sistema processuale*, in *Giur. it*., 2018, f. 6, p. 1779), forniti periodicamente, pubblicamente e gratuitamente da coloro che producono captatori informatici (S. ATERNO, *Il punto di vista degli operatori. Il difensore*, p. 322).

[178] Così come non sono previste particolari forme per il conferimento dell'incarico di ausiliario né è richiesto l'impiego di una forma scritta. Nonostante ciò, la giurisprudenza ha optato per la legittimità dei risultati appresi. Cass., sez. III, 18 febbraio 2010, n. 17177, in *C.E.D. Cass*., n. 246978; sez. III, 5 marzo 2009, n. 16683, *ivi,* n. 243462.

esigenze di pubblica sicurezza»[179] e non certo senza limiti spazio-temporali, «generando nell'interessato un sentimento di soggezione ad una costante sorveglianza»[180].

In conclusione, può ritenersi che la costruzione dei confini operativi del captatore informatico sia determinata da propositi condivisibili ma i risultati sono destinati ad essere inefficaci. Un buon governo di questo comparto avrebbe dovuto tener conto del cambiamento sostanziale del sistema intercettativo: se si ritenesse che oggi alcuni interessi rilevanti corrono un rischio insopportabile, sarebbe doveroso un intervento coordinato di riassetto normativo per una efficace tutela e, invece, sorprendentemente, il quadro normativo esistente non prevede regole confortate da sanzioni[181].

---

[179] Così Corte di giustizia UE, 8 aprile 2014, *Digital Rights Ireland Ltd* contro *Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung e a.*, in *www. eur-lex.europa.eu*. Con tale pronuncia la Corte ha dichiarato invalida la Direttiva 2006/24/EC sulla conservazione dei dati, a seguito di rinvio pregiudiziale presentato sia dalla *High Court* irlandese che dalla *Verfassungsgerichtshof* (Corte costituzionale) austriaca in merito proprio alla validità di tale direttiva, con particolare riferimento ai diritti fondamentali del rispetto della vita privata e della protezione dei dati personali, sanciti entrambi dalla Carta dei diritti fondamentali dell'Unione Europea. Tale Corte ha osservato anzitutto che i dati da conservare consentono, in particolare, di conoscere l'identità della persona con la quale un utente registrato ha comunicato e con quali mezzi; identificare il momento e il luogo della comunicazione; conoscere la frequenza delle comunicazioni dell'utente con determinate persone in uno specifico periodo. Tali dati, nel complesso, possono fornire informazioni molto precise sulla vita privata delle persone i cui dati sono conservati, come ad esempio le abitudini della vita quotidiana, i luoghi di residenza, i movimenti, le attività svolte, le relazioni sociali e gli ambienti frequentati. In merito a ciò, ha ritenuto che, imponendo la conservazione di tali dati e permettendo alle autorità nazionali competenti di accedere a tali dati, la direttiva interferisce in modo eccessivo con i diritti fondamentali del rispetto della vita privata e della protezione dei dati personali. Inoltre, il fatto che i dati siano conservati e utilizzati senza che l'utente ne sia previamente informato, può ingenerare negli interessati un sentimento di soggezione a una costante sorveglianza. Sul tema, si rinvia a Cap. IV.

[180] Cass., sez. un., 28 aprile 2016, n. 26889, cit.

[181] Cfr. T. BENE, *"Il re è nudo": anomie disapplicative a proposito del captatore informatico*, cit., p. 8. L'Autrice evidenzia anche che «[L]l'indirizzo giurisprudenziale consolidato, infatti, riteneva che l'inosservanza delle disposizioni previste dall'art. 89 disp. att. c.p.p., in tema di verbali e nastri registrati delle intercettazioni, non determinasse l'inutilizzabilità degli esiti dell'attività captativa legittimamente disposta ed eseguita». Cfr. Cass., sez. I, 2 dicembre 2009, n. 8836, in *C.E.D. Cass*., n. 246377; sez. IV, 17 settembre 2004, n. 49306, *ivi*, n. 229922; sez. IV, 14 gennaio 2004, n. 17574, *ivi*, n. 228173; sez. VI, 26 ottobre 1993, n. 11421, *ivi,* n. 198560. Più di recente, sez. V, 19 gennaio 2018, n. 15472, cit.; sez. III, 17 febbraio 2015, n. 20418, in *Cass. pen.,* 2016, f. 1, p. 313. Come sottolineato, tale orientamento appare ancora attuale, non essendo stato aggiornato l'art. 271, comma 1, c.p.p. Sul tema, N. GALANTINI, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina*, cit., p. 227 ss.

CAPITOLO IV

L'IMPATTO SUI DIRITTI FONDAMENTALI

SOMMARIO: 1. Le potenzialità intrusive del *virus* alla prova dei diritti fondamentali: considerazioni dogmatiche – 2. Il diritto alla segretezza della corrispondenza e delle comunicazioni quale oggetto di tutela costituzionale e convenzionale – 3. L'inviolabilità del domicilio: il complesso adeguamento della nozione al diritto vivente – 4. Il diritto alla riservatezza e alla *privacy* nel quadro dei diritti fondamentali – 4.1. *Segue*: la tutela della *privacy* nel diritto positivo – 5. L'innovazione tecnologica e i diritti di "terza generazione". Dal domicilio informatico all'intangibilità della vita digitale – 6. Sicurezza *vs* libertà: alla ricerca di un difficile equilibrio

1. LE POTENZIALITÀ INTRUSIVE DEL *VIRUS* ALLA PROVA DEI DIRITTI FONDAMENTALI: CONSIDERAZIONI DOGMATICHE

Senza dubbio, l'intercettazione di comunicazioni e conversazioni costituisce «un'intrusione nella vita privata e nello specifico della corrispondenza»[1], «da ritenersi, in via di principio, non auspicabile e difficilmente compatibile in una società democratica»[2].

In effetti, nelle trattazioni dottrinali, così come nelle pronunce giurisprudenziali aventi ad oggetto il tema delle intercettazioni, l'analisi dei profili costituzionali ruota intorno all'art. 15 Cost., inerente al diritto di comunicare liberamente, all'art. 14 Cost., preordinato a garantire

[1] Corte EDU, Grande Camera, 6 settembre 1978, *Klass c. Germania*, n. 5029/71, § 41. Nello stesso senso, *ex pluribus*, Corte EDU, sez. II, 10 aprile 2007, *Panarisi c. Italia*, n. 46794/99; sez. II, 31 maggio 2005, *Vetter c. Francia*, 59842/00; Grande Camera, 16 dicembre 1992, *Niemietz c. Germania*, n. 13710/88, § 32. In dottrina, V. MASI, *Le intercettazioni tre frizioni interne e giurisprudenza della Corte di Strasburgo*, in *Dir. pen. proc.,* 2011, p. 1159. Da ultimo, D. CURTOTTI, *Le intercettazioni e la giurisprudenza europea*, in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci, 2018, p. 3 ss.

[2] Così Corte EDU, Grande Camera, 2 agosto 1984, *Malone c. Regno Unito*, n. 8691/79, § 67, in *Publications of the European Court of Human Rights*, vol. 82, p. 37 ss. Il principio è stato ribadito anche in diverse successive pronunce. Corte EDU, sez. IV, 18 maggio 2010, *Kennedy c. Regno Unito*, n. 26839/05, § 118–129 e 151. Non va, tuttavia, sottaciuta la centralità del mezzo di ricerca della prova in esame nel panorama investigativo. Come sostenuto, "[L]l'intercettazione, quale atto a sorpresa per natura irripetibile, consente di pervenire a risultati di particolare interesse investigativo, ai fini della conduzione delle indagini e delle successive determinazioni inerenti all'esercizio dell'azione penale, ma, soprattutto, di rilevante attitudine probatoria ai fini dell'accertamento del fatto processuale". Così L. KALB, *Meccanismi operativi e regole procedurali*, in AA. VV., *Le intercettazioni di conversazioni e comunicazioni. Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti*. Atti del Convegno 5-7 ottobre 2007, Giuffrè, 2009, p. 277 ss. Sul tema anche O. CALAVITA, *L'odissea del* trojan horse. *Tra potenzialità tecniche e lacune normative,* in *Dir. pen. cont.,* 2018, n. 11, p. 51 ss. È stato altresì rilevato che anche il giurista «da giurista umanista tende ad assumere le vesti di "giurista tecnologico"» Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* Giappichelli, 2018, p. 11. Nello stesso senso A. ZAMPAGLIONE, *Il recupero della funzione di garanzia del decreto autorizzativo quale "strada maestra" per arginare le potenzialità invasive del* trojan *e salvaguardare valori di rilievo costituzionale*, in *www.dirittifondamentali.it*, 2019, p. 1 s.

l'inviolabilità del domicilio da indebite intrusioni[3], nonché all'art. 8 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali[4], concernente la tutela della privatezza e della riservatezza[5].

[3] Sui rapporti tra le intercettazioni e i principi costituzionali di cui agli artt. 14 e 15 Cost., la dottrina è assai ampia. Durante la vigenza del Codice del 1930, G. AMATO, *Individuo e autorità nella disciplina della libertà personale*, Giuffrè, 1976, *passim*; A. BARBERA, *I principi costituzionali della libertà personale*, Giuffrè, 1971, p. 88 ss.; P. BARILE, *Diritti dell'uomo e libertà fondamentali*, Il Mulino, 1984; G. CONSO, *Processo penale e Costituzione: dodici anni di pagine sparse*, Giuffrè, 1969; L. GRANATA, *Le intercettazioni telefoniche nel nostro codice di procedura penale*, in *Riv. polizia*, 1961, p. 449 ss.; P. GROSSO, voce *Intercettazioni telefoniche*, in *Enc. dir.,* XXI, Giuffrè, 1971, p. 889 s.; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, Milano, 1983, p. 187 ss. A seguito dell'entrata in vigore del Codice del 1988, P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. pen.,* VII, Utet, 1993, p. 183 ss.; A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996, p. 44 ss.; G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir*., VI, Giuffrè, 2013, p. 748 ss.; L. FILIPPI, *L'intercettazione di comunicazioni*, Giuffrè, 1997, 16 ss.; C. FRANCHINI, voce *Intercettazione di comunicazioni*, in *Enc. giur*., Treccani, 1988, p. 1 ss.; G. FUMU, sub *artt. 266–271*, in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, 1990, p. 774; A. GAITO, *In tema di intercettazioni delle conversazioni in abitazioni private*, in *Giur. it*., 1991, f. II, p. 466 ss.; A. PACE, *Problematiche delle libertà costituzionali*, Cedam, 1992, p. 214 ss.; D. POTETTI, *Corte costituzionale n. 81/1993: la forza espansiva della tutela accordata dall'art. 15, comma 1 della Costituzione*, in *Cass. pen.,* 1993, f. 11, p. 2746 ss.; A. SCELLA, *Dubbi di legittimità costituzionale e questioni applicative in tema di intercettazioni ambientali compiute in luogo di privata dimora*, in *Cass. pen*., 1995, f. 10, p. 992 ss.; A. LOIODICE, *Libertà di comunicazione e principi costituzionali*, in AA. VV., *Informazione e telecomunicazione*, a cura di R. Zaccaria, in *Trattato di diritto amministrativo*, diretto da G. Santaniello, Cedam, 1999, p. 7 ss. Più di recente, E. APRILE, *Intercettazioni di comunicazioni*, in AA. VV., *Prove,* a cura di A. Scalfati, in *Trattato di procedura penale*, diretto da G. Spangher, Utet, 2009, p. 475 ss.; E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche e ambientali*, *Innovazioni tecnologiche e nuovi questioni giuridiche*, Giuffrè, 2004, p. 6 ss.; A. BALSAMO, *Intercettazioni: gli* standards *europei, la realtà italiana, le prospettive di riforma,* in *Cass. pen.,* 2009, n. 10, p. 4023 ss.; M. BRANCACCIO, sub *art. 266,* in *Codice di procedura penale,* a cura di G. Canzio–R. Bricchetti, Giuffrè, 2017, p. 1987 ss.; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. disc. pen*., X, Utet, 2001, p. 175 ss.; C. BERTOSSI, *Intercettazioni ambientali e tutela della libertà domiciliare,* in *Dir. pen. proc*., 2004, n. 7, p. 869 ss.; M. BONETTI, *Riservatezza e processo penale*, Giuffrè, 2003, p. 256 ss.; P. CARETTI, *I diritti fondamentali,* Torino 2005; C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in *www.forumcostituzionale.it*, 21 ottobre 2013, p. 10 ss.; A. DIDDI, *L'inviolabilità della segretezza delle comunicazioni*, in AA. VV., *Processo penale e costituzione*, a cura di F.R. Dinacci, Giuffrè, 2010, p. 268 ss.; C. DI MARTINO, *Le intercettazioni ambientali*, in *Ind. pen*., 2003, n. 3, p. 1149 ss.; L. FILIPPI, sub *art. 266*, in *Codice di procedura penale commentato*, a cura di A. Giarda–G. Spangher, V ed., Wolter Kluwers, 2017, p. 2547 ss.; ID., *Intercettazioni, tabulati e altre limitazioni alla segretezza delle comunicazioni,* in AA. VV., *Procedura penale. Teoria e pratica del processo*, diretto da G. Spangher–A. Marandola–G. Garuti–L. Kalb, Utet, 2015, p. 1118 ss.; ID., voce *Intercettazioni telefoniche (diritto processuale penale),* in *Enc. dir*., VI, Giuffrè, 2002, p. 565; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007, p. 56 ss.; E. MILITELLO, *Limiti alla segretezza delle comunicazioni e prevenzione dei reati di terrorismo nell'ordinamento federale statunitense*, in *Ind. pen.,* 2017, n. 2, p. 623 ss.; G. SILVESTRI, *L'individuazione dei diritti della persona*, *Relazione presentata al XXXII Convegno dell'Associazione tra gli studiosi del processo penale* "*Prof. G.D. Pisapia*", intitolato "*Diritti della persona e nuove sfide del processo penale*", tenutosi a Salerno dal 25 al 27 ottobre 2018, in *Dir. pen. cont.*, 29 ottobre 2018, p. 8 s.; G. SPANGHER, *Le criticità della disciplina delle intercettazioni telefoniche,* in *Dir. pen. proc.*, 2016, f. 3, p. 921 ss.; A. VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Cedam, 2011, p. 40 ss. Con precipuo riguardo alle intercettazioni tramite captatore informatico, A. CAPONE, *Intercettazioni e costituzione. Problemi vecchi e nuovi*, in *Cass. pen*., 2017, f. 3, p. 1263 ss.; C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* in *Dir. pen., proc*., 2018, f. 8, p. 1210 ss.; O.

La *quaestio* relativa all'impatto delle attività captative rispetto ai precetti fondamentali diventa assai più preoccupante allorquando le Forze di polizia, nell'espletamento delle loro funzioni, si servono di strumenti investigativi ad alto contenuto tecnologico, non sempre di agevole classificazione, il cui utilizzo risulta necessario a rendere effettiva la lotta contro gravi e sempre più evolute forme di criminalità.

Più precisamente, le operazioni condotte attraverso l'ausilio del captatore informatico coinvolgono un catalogo di diritti assai più ampio e variegato rispetto a quelli interessati dalla "mera" captazione di conversazioni e comunicazioni tra presenti, dal momento che è la stessa idea di libertà personale ad essere compromessa da un utilizzo perdurante dello strumento inoculato su un qualsiasi apparecchio informatico di uso quotidiano: in ipotesi del genere, infatti, l'attività d'indagine espletata si tramuterebbe in una forma di sorveglianza occulta e continuativa del *device* e di chi lo usa[6].

Di qui, appare chiara l'esigenza di estendere il campo di indagine ad altri valori costituzionali che risultano altrettanto suscettibili di compressione secondo l'atteggiarsi delle diverse modalità

MAZZA, *Amorfismo legale e adiaforia costituzionale nella nuova disciplina delle intercettazioni*, in *Proc. pen. giust.,* 2018, f. 4, p. 683 ss.

[4] La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) è stata firmata a Roma il 4 novembre 1950 e resa esecutiva nell'ordinamento interno con l. 4 agosto 1955, n. 848, recante "*Ratifica ed esecuzione della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali firmata a Roma il 4 novembre 1950 e del Protocollo addizionale alla Convenzione stessa, firmato a Parigi il 20 marzo 1952*", in *www.gazzettaufficale.it.* Fra i primi commentatori, M. CHIAVARIO, *La Convenzione europea dei diritti dell'uomo nel sistema delle fonti normative in materia penale,* Giuffrè, 1969; G. GREMENTIERI, *L'Italia e la Convenzione europea dei diritti dell'uomo*, Giuffrè, 1989. Più di recente, S. BARTOLE–B. CONFORTI–G. RAIMONDI, *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Cedam, 2012; A. DI STASI*, Introduzione alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Cedam, 2016; ID., *Cedu e ordinamento interno: la giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno*, 2010–2015, Cedam, 2016.

[5] *Ex plurimis,* G. ARCUDI–V. POLI, *Il diritto alla riservatezza*, Ipsoa, 2000, p. 5 ss.; D. BOLOGNESI, *La disciplina sulle intercettazioni a fronte della Convenzione per la salvaguardia dei diritti dell'uomo*, in *Dir. pen. proc.,* 1996, f. 12, p. 1528 ss.; A. BALSAMO–A.T. TAMIETTI, *Le intercettazioni, tra garanzie formali e sostanziali*, in AA. VV., *Giurisprudenza europea e processo penale italiano*, a cura di A. Balsamo–R.E. Kostoris, Giappichelli, 2008, p. 427 ss.; M. BONETTI*, Riservatezza e processo penale,* cit., p. 126 ss.; G. BUSIA, *Così la riservatezza "guadagna" terreno*, in *Guida dir*., 2004, f. 10, p. 58 ss.; A. CATAUDELLA, voce *Riservatezza (diritto alla)*, in *Enc. giur,* XXVII, Treccani, 1991, p. 1 ss.; S. FIORE, voce *Riservatezza (diritto alla),* in *Enc. giur.,* XXVII, Treccani, 1998, p. 3 ss.; S. FURFARO, voce *Riservatezza*, in *Dig. disc. pen*., VI, Utet, 2008, p. 1066 ss.; ID., *Un problema irrisolto: le intercettazioni telefoniche*, in AA. VV., *Procedura penale e garanzie europee,* a cura di A. Gaito, Giappichelli, 2006, p. 122 ss.*;* G. MAROTTA*, Innovazioni tecnologiche e diritto al rispetto del domicilio nella Convenzione europea*, in *Riv. dir. internaz*., 2005, f. 4, p. 1043 ss.; A. PACE, *Nuove frontiere della libertà di comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza)?,* in *Giur. cost.,* 1993, p. 747 ss. Più di recente, M. DANIELE, *Intercettazioni ed indagini informatiche*, in AA. VV., *Manuale di procedura penale europea*, a cura di R.E. Kostoris, 2017, Giuffrè, p. 429 ss.; A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in AA. VV., *Principi europei del processo penale*, a cura di A. Gaito, Dike, 2016, p. 363 ss.; A. GALLUCCIO, sub *art. 8 Cedu. Profili generali sugli artt. 8–11 CEDU*, in AA. VV., *Corte di Strasburgo e Giustizia penale*, a cura di G. Ubertis–F. Viganò, Giappichelli, 2016, p. 255; O. MAZZA, *CEDU e diritto interno,* in AA. VV., *I principi europei del processo penale*, cit., p. 4 ss.

[6] Al riguardo, sono attuali le considerazioni di V. GREVI, *Libertà personale dell'imputato e Costituzione*, 1976, Giuffrè, p. 2: «il diritto alla libertà personale, atteso il carattere peculiare e primordiale dell'interesse che vi è garantito, si configura nel sistema come presupposto di tutti gli altri diritti di libertà, in quanto logicamente li precede e li condiziona a livello operativo, rendendone possibile la piena esplicazione».

investigative[7]. A ben guardare, infatti, il costante ricorso a tali evoluti sistemi di supervisione e controllo da remoto non solo determina la violazione dei diritti di "prima" e "seconda" generazione[8], ma comporta anche la proliferazione di minacce a precetti di "terza" generazione, propri di una "società 2.0", atti a tutelare le nuove esigenze di un individuo informatizzato e impongono un salto qualitativo nell'individuazione di norme volte a garantirlo[9].

Ecco, quindi, che la diffidenza di fronte all'utilizzo di tali strumenti investigativi diventa sempre più crescente e, nonostante lo stato dell'arte si profili assai critico, il legislatore scientemente decide di non rispondere alle sollecitazioni internazionali che richiedono l'introduzione di una disciplina più puntuale dell'istituto in esame[10], al fine di fugare

---

[7] Come precisa L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale,* in *Proc. pen. giust*., 2020, f. 2, p. 291, «[L]l'ormai diffuso utilizzo di tecnologie digitali apre la via a moderne modalità investigative, che trovano un necessario limite nel rispetto delle libertà delle persone coinvolte. Sono libertà che se, da un lato, possono essere ricondotte ai principi costituzionali tradizionalmente in gioco nel procedimento penale, dall'altro lato, chiamano in causa garanzie inedite, a presidio di una "nuova" sfera di intimità da proteggere». Secondo A. CAPONE, *Intercettazioni e costituzione. Problemi vecchi e nuovi*, cit., p. 1268, «[…] l'uso di queste forme di intrusione nell'oggetto che racchiude gran parte della vita privata senza dubbio ha un'idoneeità lesiva nuova». Nello stesso senso L. PICOTTI, *Spunti di riflessione per il penalista della sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen*., 2016, p. 9.

[8] Secondo N. BOBBIO, *L'età dei diritti*, Milano, 2005, p. 155, sono diritti di "seconda generazione", la *privacy* e la riservatezza. Sul punto, v. § ?.

[9] Come di recente sostenuto, «[S]sono numerosi ed eterogenei i "diritti senza legge", che oggi non si possono ignorare, in ossequio ad un malinteso positivismo, che sfocia spesso in mero testualismo». Così G. SILVESTRI, *L'individuazione dei diritti della persona*, cit., p. 7. Nello stesso senso, A. MORELLI, *I diritti senza legge*, in *www.giurcost.org*, 2015, f. I, p. 23 ss. Inoltre, è stato affermato che «i diritti fondamentali sono oggetto di tutela "progressiva" non solo nel senso di un loro opportuno adeguamento all'evoluzione tecnologica e alle sfide del tempo, ma altresì per il fatto di trovarsi in rapporto di costante tensione con l'esigenza – anch'essa di rango costituzionale – di un efficace perseguimento dei reati». Così R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.,* 2014, f. 3, p. 1134 ss. In relazione ai "nuovi" diritti emergenti in ragione del progresso tecnologico, più in generale, A. BARBERA, *"Nuovi diritti": attenzione ai confini*, in AA. VV., *Corte costituzionale e diritti fondamentali*, a cura di L. Califano, Giappichelli, 2004, p. 28 ss.; C. CARUSO, *L'individuo nella rete: i diritti della persona al tempo di Internet*, in AA. VV., *Desafios para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologias*, a cura di G.M. Teruel Lozano–A.P. Rez Miras–E.C. Raffiotta, Aranzadi, 2013, p. 22 ss.; V. DE FLAMMINEIS, *Le intercettazioni telematiche*, in *Dir. pen. proc.,* 2013, f. 2, p. 989 ss.; R. FLOR, *Nuove tecnologie e giustizia penale in Europa tra esigenze di accertamento e prevenzione dei reati e quelle di tutela della riservatezza: il ruolo "propulsore" della Corte di Giustizia*, in *Studi in onore di Maurizio Pedrazza Gorlero*, ESI, 2014, p. 247 ss.; ID., *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Dir. pen. cont*., 20 settembre 2012; L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. merito*, 2012, p. 2532 ss.; ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in AA. VV., *Il diritto penale dell'informatica all'epoca di internet*, a cura di L. Picotti, Cedam, 2004, p. 87 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 49 ss. Con precipuo riguardo al tema del captatore, C. CONTI, *Prova informatica e diritti fondamentali: a proposito di "captatore" e non solo*, in *Dir. pen. proc*., 2018, f. 9, p. 1210 ss.; ID., *Le nuove norme sulla riservatezza delle intercettazioni: anatomia di una riforma discussa,* in *Giur. it.,* 2018, f. 7, p. 1754 ss.; M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali,* in *Dir. pen. proc*., 2015, f. 9, p. 1168 ss.

[10] Suscitano molto clamore, oltre che penetranti riflessioni sulla tenuta del sistema penale italiano in materia, le condanne europee dell'Italia per violazione dell'art. 8 CEDU. Dal 1959 al 2017, le sentenze di condanna sono state 163; seconde solo alla Repubblica Russa (171) e molto lontane da tutti gli altri Stati (terza, per numero di condanne, è la Polonia con 113). Nel solo 2017, le condanne a carico

definitivamente i numerosi sospetti di illegittimità da sempre ingenerati ma acuiti dallo "smodato" uso della tecnologia.

Nel marasma che di recente ha colpito la disciplina delle intercettazioni, si avverte come persa l'occasione per una ridefinizione costituzionalmente orientata delle altre attività (diverse dall'intercettazione ambientale) che il captatore, almeno in potenza, è in grado di svolgere. Probabilmente il legislatore nazionale preferisce tacere più che normare, lasciare agli interpreti del diritto l'arduo compito di definire i limiti e la portata dell'istituto piuttosto che fornire criteri e parametri di legalità per indirizzare le scelte dei pratici, consapevole che le ingerenze ai diritti fondamentali non hanno alcuna ripercussione in sede procedimentale in ragione dell'inutilizzabilità dei dati raccolti *ulta vis*, disattendendo, così, i dettami della giurisprudenza europea la quale, per contro, ritiene che «[O]gni intromissione riveste di per sé la caratteristica di ingerenza della pubblica autorità nella sfera privata e ciò anche quando di essa non si sia fatto un uso processualmente rilevante»[11].

2. Il diritto alla segretezza della corrispondenza e delle comunicazioni quale oggetto di tutela costituzionale e convenzionale

La libertà di comunicare riservatamente è «corollario indispensabile di una ben intesa libertà individuale e, insieme a quella personale, di domicilio e di espressione, elemento fondante il nucleo intangibile della persona umana»[12].

---

del nostro Stato sono state 7. Cfr. D. CURTOTTI, *Le intercettazioni e la giurisprudenza europea*, cit., p. 3.

[11] Così Corte EDU, Grande Camera, 25 marzo 1998, *Kopp c. Svizzera*, n. 23224/94, § 53 s. Ma già Grande Camera, 15 giugno 1992, *Ludi c. Svizzera*, n. 12433/86.

[12] Si esprime così, seppur in riferimento al diritto di comunicare liberamente e segretamente in epoca statutararia, F. RACIOPPI–I. BRUNELLI, *Commento allo Statuto del Regno,* II, Unione tipografico-editrice, 1909. Nello stesso senso, anche S. ROMANO, *Il diritto pubblico italiano,* Giuffrè, 1988, p. 27, secondo cui «la libertà personale, la libertà di domicilio e la libertà di corrispondere segretamente [sono riconducibili] ad un unico […] diritto di libertà, che nonostante le varie, indefinite manifestazioni di cui è suscettibile, […] [era] da concepirsi come un diritto unitario, avente per oggetto l'indipendenza personale di fronte allo Stato e la sua difesa contro le illegittime invadenze di quest'ultimo». Tale concezione non sembra essere smentita dall'esegesi dell'attuale assetto normativo di cui all'art. 15 Cost. Infatti, dall'analisi dei lavori preparatori emerge che il contenuto della libertà di comunicare segretamente si pone «al pari della libertà domiciliare garantita dall'art. 14 Cost. come un ampliamento ed una precisazione del fondamentale principio di inviolabilità della persona umana sanzionato dall'art. 13 Cost.». Così P. BARILE–E. CHELI, voce *Corrispondenza (libertà di),* in *Enc. dir*., X, Giuffrè, 1962, p. 744. A tal proposito va detto che inizialmente la I Sottocommisione ritiene indispensabile separare, almeno topograficamente, i tre articoli, in modo da attribuire agli stessi un carattere autonomo. Nella seduta della "Commissione plenaria dei 75", su proposta dell'On. Perassi, si decide di tornare all'originaria formulazione e di dedicare alla libertà in esame un articolo a sé stante, con la rilevante esclusione della norma relativa alle limitazioni in tempo di guerra. Cfr. Atti Assemblea Costituente, Resoconto stenografico, 1947, p. 169 s. Inoltre, non può sottacersi l'inscindibile nesso esistente tra gli artt. 2 e 15 Cost., in quanto la libertà di comunicare riservatamente può essere considerata «come proiezione spirituale della persona, naturale completamento della tutela che la Costituzione offre alla sua proiezione spaziale (art. 14 Cost.), alla libertà in senso fisico (art. 13 Cost.) e, in particolare, alla dignità umana». Così C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, cit., p. 4. Ma già, V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* Giuffrè, 1963, p. 41, per cui «[I]il complesso delle libertà costituzionali forma, per così dire, quasi un tessuto, e nel contesto delle singole disposizioni vi sono delle categorie, delle sottospecie, dei rapporti, e delle linee di "derivazione" del principio fondamentale dell'art. 2 della Costituzione». In questo senso anche la

Il precetto in esame rappresenta, in sostanza, il fulcro di quel complesso dei diritti della personalità[13] cui la Carta costituzionale riconosce il carattere dell'inviolabilità[14].

giurisprudenza costituzionale. Cfr. Corte cost., 23 luglio 1991, n. 366, in *Giur. cost*., 1991, p. 3261 ss., che così si esprime «[…] l'esigenza di amministrare la giustizia e, in particolare, quella di reprimere i reati corrisponda a un interesse pubblico primario, costituzionalmente rilevante, il cui soddisfacimento è assolutamente inderogabile. Allo stesso modo, non si può dubitare che tale interesse primario giustifichi anche il ricorso a un mezzo dotato di formidabile capacità intrusiva, quale l'intercettazione telefonica. Tuttavia, proprio perché si tratta di uno strumento estremamente penetrante e in grado di invadere anche la *privacy* di soggetti terzi, del tutto estranei ai reati per i quali si procede, e proprio perché la Costituzione riconosce un particolare pregio all'intangibilità della sfera privata negli aspetti più significativi e più legati alla vita intima della persona umana, le restrizioni alla libertà e alla segretezza delle comunicazioni conseguenti alle intercettazioni telefoniche sono sottoposte a condizioni di validità particolarmente rigorose, commisurate alla natura indubbiamente eccezionale dei limiti apponibili a un diritto personale di carattere inviolabile, quale la libertà e la segretezza delle comunicazioni (art. 15 della Costituzione)». In dottrina, G. AMATO, *Commento all'art. 14 Cost.,* in *Commentario della Costituzione*, a cura di G. Branca, Il Mulino, 1977, p. 62 ss.; T.A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, 1978, p. 46 ss.; A. BALDASSARRE, voce *Diritti inviolabili*, in *Enc. giur.,* Treccani, XI, 1989, p. 28 ss.; P. BARILE–E. CHELI, voce *Domicilio (libertà di*), in *Enc. dir.,* XIII, Giuffrè, 1964, p. 865 ss.; T. MARTINES, *Diritto costituzionale*, Milano, 1997, p. 703 ss. Da ultimo, G. ILLUMINATI, *Libertà e segretezza della comunicazione*, in AA. VV., *Diritti della persona e nuove sfide del processo penale,* Giuffrè, 2019, p. 155 ss.

[13] La categoria in esame si caratterizza per avere ad oggetto facoltà non create dal diritto positivo ma da questo riconosciute e protette. Cfr. Corte cost., 27 aprile 1972, n. 77, in *Giur. cost*., 1972, p. 1061. La dottrina sul punto è assai copiosa. Senza pretese di completezza, G. AMATO, *Commento all'art. 14 Cost.,* in *Commentario della Costituzione*, cit., p. 62 ss.; T.A. AULETTA, *Riservatezza e tutela della personalità*, cit., p. 46 ss.; A. BALDASSARRE, voce *Diritti inviolabili*, cit., p. 28 ss.; P. BARILE–E. CHELI, voce *Domicilio (libertà di*), cit., p. 865 ss.; G. BOGNETTI, voce *Diritti dell'uomo,* in *Dig, disc. priv*., V, Utet, 1989, p. 383 ss.; G. FLICK, *Globalizzazione e diritti umani*, in *Jus*, 2000, p. 172 ss.; D. MESSINETTI, voce *Personalità (diritti della),* in *Enc. dir*., XXXIII, Giuffrè, 1983, p. 355 ss. In chiave comparatistica, M. PATRONO, *I diritti dell'uomo nel paese d'Europa*, Cedam, 2000, p. 23 ss.

[14] Vale a dire un diritto caratterizzato dalla «coessenzailità rispetto alla forma di Stato vigente in Italia». Così L. PALADIN, *Diritto costituzionale*, Cedam, 1994, p. 564.

Sotto il profilo sistematico, l'art. 15 Cost.[15] sembra assolutamente logico e coerente nel distinguere l'oggetto e la portata della tutela apprestata (comma primo) dal complesso di garanzie atte a preservare i valori *ivi* contemplati da indebite interferenze (comma secondo)[16].

[15] Pur nascendo come situazione giuridica regolante esclusivamente i rapporti tra i privati – quale pretesa a che il contenuto di una corrispondenza epistolare rimanesse segreto ai soggetti terzi (Cfr. G. AMATO, voce *Libertà (dir. cost.),* in *Enc. dir*., XXIV, Giuffrè, 1974, p. 272 ss.) – è assai curiosa l'assenza di una disposizione di tutela della libertà della corrispondenza e di ogni altra forma comunicativa all'interno dello Statuto albertino del 1848. E ciò per almeno due ordini di ragioni. Intanto in Francia, all'indomani della rivoluzione del 1848, la libertà di comunicare segretamente trova una duplice tutela: la legge 10–11 giugno 1791 per un verso abolisce i *Cabinets noirs,* per un altro afferma solennemente che «*le secret des lettres est inviolable, et, sous aucun prétexte, il ne peut y etre porté atteinte, ni par les individus, ni par les corps administratifs*». Inoltre, le altre costituzioni pressoché coeve allo Statuto dispongono di norme poste a tutela della libertà predetta (vedasi la Costituzione belga del 1831, *ex* art. 22, olandese del 1814, *ex* art. 154, e prussiana, *ex* art. 33). In Italia, la Costituzione del Regno delle Due Sicilie del 1848 dispone all'art. 29 che «il segreto delle lettere è inviolabile. La responsabilità degli agenti della posta, per la violazione del segreto delle lettere, sarà determinata da una legge». Sulla situazione vigente all'epoca statutaria, G. MARANINI, *Le origini dello Statuto Albertino,* Vallecchi editore, 1926, p. 191 ss. Per una ricostruzione del periodo storico in esame, U. GUSPINI, *L'orecchio del regime. Le intercettazioni telefoniche al tempo del fascismo*, Mursia editore, 1973; M. PISANI, *La tutela personale della "riservatezza". Aspetti processuali*, in *Riv. it. dir. proc. pen*., 1967, p. 793 ss. L'avvento della Costituzione repubblicana, per contro, appresta un efficace complesso di garanzie, idoneo ad assicurare la tutela dei diritti di libertà individuali e collettivi che nelle epoche precedenti avevano goduto di insufficiente protezione. Memori di tale insegnamento, i costituenti danno vita ad una Costituzione rigida nella quale i valori di maggiore rilevo sono tutelati attraverso le previsioni della riserva di legge e di giurisdizione, volte, rispettivamente, all'attribuzione alla legge del monopolio normativo e al conferimento all'autorità giudiziaria del potere in ordine alla valutazione dei presupposti per l'adozione di atti, debitamente motivati, su di essa incidenti. Per un'esegesi storica del diritto di cui all'art. 15 Cost., A. BARBERA, *Le basi filosofiche del costituzionalismo: lineamenti di filosofia del diritto costituzionale,* in AA. VV., *Le basi filosofiche del costituzionalismo: lineamenti di filosofia del diritto costituzionale,* a cura di A. Barbera, Laterza, 2000, p. 3 ss.; P. CARETTI, voce *Comunicazione e informazione*, in *Enc. dir.,* I, Giuffrè, 2007, p. 220 ss.; ID., *I diritti fondamentali,* cit., p. 42 ss.; ID., voce *Corrispondenza (libertà di,)* in *Dig. disc. pubbl.,* IV*,* Utet, 1989, p. 201 ss.; C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, cit., p. 1 ss.; N. MATTEUCCI, *Lo Stato moderno*, Il Mulino, 1997, p. 15 ss.

[16] Sulla portata della garanzia costituzionale delle comunicazioni riservate, la dottrina si presenta assai vasta. *Ex multis,* P. BARILE–E. CHELI, voce *Corrispondenza (libertà di),* cit., p. 743 s.; P. BARILE, *Diritti dell'uomo e libertà fondamentali,* cit., p. 163 s.; M. BETZU, *Comunicazione, manifestazione del pensiero e tecnologie polifunzionali,* in *Quad. Cost.,* 2006, n. 3, p. 511 ss.; P. CARETTI, *I diritti fondamentali,* cit., p. 44 ss.; P. COSTANZO, voce *Internet,* in *Dig. disc. pubbl*., I, Utet, 2000, p. 347 s.; ID., *La circolazione dell'informazione giuridica digitalizzata: fenomenologia e profili problematici,* in *Dir. Inf*., 1999, p. 579 s.; ID., *Profili costituzionali delle telecomunicazioni*, in AA. VV., *La disciplina giuridica delle telecomunicazioni*, a cura di F. Bonelli–S. Cassese, Giuffrè, 1999, p. 3 s.; F. DONATI, sub *art. 15,* in *Comm. Cost. it*., a cura di R. Bifulco–A. Celotto–M. Olivetti, Cedam, 2006, p. 362 s.; E. GIANFRANCESCO, *Profili ricostruttivi della libertà e segretezza di corrispondenza e comunicazione,* in *Dir. e società*, 2008, p. 219 s.; R. GUARINIELLO, *Rapporti tra amministrazione postale e autorità giudiziaria in tema di libertà e segretezza della corrispondenza*, in *Giur. cost.,* 1968, p. 1592 s.; V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* cit.; ID., *La libertà di corrispondenza*, in AA. VV., *La pubblica sicurezza*, a cura di P. Barile, Neri Pozza, 1967, p. 203 s.; P. LOGROSCINO, *Libertà di comunicare e convergenza multimediale*, Pensa editore, 2008; A. LOIODICE, *Libertà di comunicazione e principi costituzionali*, cit., p. 3 s.; A. PACE, *L'ordinamento della comunicazione*, in *Dir. pubbl.,* 2004, p. 841; ID., *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza)?,* in *Giur. cost*., 1993, p. 742 ss.; ID., *Libertà di comunicare riservatamente*, in AA. VV., *Problematica delle libertà costituzionali,* II, a cura di A. Pace, Cedam, 1992, p. 241 s.; G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della*

In relazione al primo aspetto, va chiarito che l'art. 15, comma 1 Cost., tutela due situazioni distinte ma complementari, ovvero «il diritto di poter comunicare e corrispondere con altri soggetti, senza che sia portata alcuna interruzione o sospensione al corso "normale" della comunicazione» (c.d. libertà in senso stretto) e «la pretesa a che soggetti diversi dai destinatari determinati non prendano illegittimamente conoscenza del contenuto della corrispondenza o di una comunicazione»[17] (segretezza).

Dunque, libertà e segretezza, «per quanto rappresentino aspetti interdipendenti del medesimo valore, conservano la propria autonomia»[18].

La libertà rappresenta la proiezione del diritto di autodeterminazione del singolo in ordine alla possibilità di entrare in contatto con altri individui o astenersene e, conseguentemente, il diritto a non subire limitazioni nel suo esercizio da interferenze esterne. La segretezza, per contro, inerisce al contenuto delle comunicazioni riservate che, in quanto tali, sono intenzionalmente sottratte dai partecipi alla conoscibilità di terzi[19].

In relazione al contenuto del precetto, ossia l'oggetto della tutela costituzionale, dall'esegesi del comma 1 dell'art. 15 Cost., si evince che la protezione è accordata sia alla corrispondenza in senso proprio che a «ogni altra forma comunicativa»[20].

---

corrispondenza, in AA. VV., *I diritti costituzionali,* a cura di R. Nania–P. Ridola, Giappichelli, 2006, p. 662; C. TROISIO, voce *Corrispondenza (libertà e segretezza della),* in *Enc. giur.,* IX, Treccani, 1988; A. VALASTRO, *L'art. 15 e i principi costituzionali sulla libertà della corrispondenza e delle comunicazioni*, in AA. VV., *Diritto della informazione della comunicazione*, a cura di R. Zaccaria, Cedam, 2004, p. 109 s.; ID., *Libertà di comunicazione e nuove tecnologie*, Giuffrè, 2001.

[17] Si esprime così V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* cit., p. 91. Nello stesso senso, P. CARETTI, *I diritti fondamentali,* cit., p. 275 ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 66 s. *Contra*, A. PACE, sub *art. 15,* cit., p. 85 ss. Sulla struttura del diritto, *amplius*, C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, cit., p. 4 ss.

[18] C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 65. Nello stesso senso, P. CARETTI, voce *Comunicazione e informazione*, cit., p. 220 s.; E. GIANFRANCESCO, *Profili ricostruttivi della libertà e segretezza di corrispondenza e comunicazione*, cit., p. 235; A. PACE, *Problematiche delle libertà costituzionali,* cit., p. 243 ss. Ma già, F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità di fatti criminosi*, in *Arch. giur.,* 1968, p. 52 s.

[19] Seppur condivisibile la concezione per cui l'art. 15 Cost. «è uno dei riferimenti utilizzabili per fondare e delimitare costituzionalmente la stessa nozione di riservatezza» (G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, in AA. VV., *I diritti costituzionali,* cit., p. 415), il diritto alla segretezza delle comunicazioni non va confuso con il diritto alla riservatezza su quanto è comunicato. Elemento distintivo della libertà di comunicare segretamente rispetto al diritto alla *privacy* è l'aspetto dinamico: vi deve essere un messaggio che un soggetto (mittente) voglia far pervenire nella sfera conoscitiva del destinatario senza che terzi ostacolino il rapporto comunicativo. La tutela della segretezza della comunicazione vuole evitare l'illegittima conoscenza del contenuto della comunicazione, «[…] mentre la tutela della riservatezza è rivolta particolarmente contro l'abuso che consegue alla legittima conoscenza sia del contenuto sia degli elementi esteriori della corrispondenza». Così V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* cit., p. 87. La segretezza è, dunque, funzionale all'azione comunicativa intersoggettiva, e solo quelle situazioni di fatto astrattamente riconducibili alla libertà di comunicare riservatamente potranno godere della riserva di giurisdizione espressamente prevista dall'art. 15 Cost. Cfr. P. BALDUCCI, *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria*, Giuffrè, 2002, p. 73 s.; A. CAMON, *Le intercettazioni nel processo penale,* cit., p. 33 ss.; F. CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, 2000, p. 64. In tema già A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione – Diritto alla riservatezza: fondamento e limiti*, in *Giur. it*., 1974, p. 616 ss.

[20] «La nozione di comunicazione consiste nello scambio di messaggi tra più soggetti, in qualsiasi modo realizzate, ad esempio tramite colloquio orale o anche gestuale […]». Così Cass., sez. IV, 19

La scelta dei costituenti è quella di fornire una nozione onnicomprensiva di comunicazione, una valvola di sfogo capace di ricomprendere «ogni atto di trasmissione del pensiero, connotato da attualità e intersoggettività, da un mittente a uno o più destinatari individuati»[21], che può avvenire «con qualsiasi mezzo che attribuisca alla comunicazione il crisma della riservatezza […]»[22].

Nonostante l'apparente chiarezza espositiva del precetto, la dottrina rileva che la nozione di "comunicazione" di cui all'art. 15 Cost., risulta così tanto ampia da apparire «ermetica e intelligibile»[23].

La *vexata quaestio* concerne la scelta di ricomprendere nella tutela di cui all'art. 15 Cost. anche le informazioni inerenti al fatto storico della comunicazione[24], oppure, aderendo ad un'interpretazione maggiormente rigorosa del *dictum*, di escludere una simile opportunità[25], dal

---

gennaio 2005, n. 11181, in *C.E.D. Cass.,* n. 231047. Nozione del tutto differente dall'usuale azione intercettativa sopra descritta, è quella di «captare immagini relative alla mera presenza di cose o persone o ai loro movimenti, non funzionali alla captazione di messaggi». Così sez. VI, 10 novembre 1997, n. 4397, in *Cass. pen.,* 1999, f. 4, p. 1188 ss. Si può notare come nella prima fattispecie lo scopo è quello di percepire sul piano uditivo ed interpretativo conversazioni, onde inferire da essi contenuti illeciti e, dunque, facilmente inquadrabile nella disciplina delle intercettazioni ambientali (artt. 266 ss.), con tutti i limiti ad esse imposte dal codice di rito. Per completezza, si rileva che la Corte Costituzionale aveva distinto tra riprese di immagini comunicative, rientranti nel genere delle intercettazioni, e riprese di mere immagini, vietate perché non disciplinate dalla legge. Cfr. Corte cost., 24 aprile 2002, n. 135, in *Giur. cost.*, 2002, p. 2176 ss. Tra le pronunce di legittimità successive successive Cass., sez. I, 29 gennaio 2003, n. 16965, in *C.E.D. Cass.,* n. 224240. Nella seconda ipotesi, invece, l'attività di indagine, prettamente visiva, è finalizzata a provare la presenza di uno o più soggetti in un determinato luogo, in un preciso momento. La giurisprudenza ritiene che, in questa seconda ipotesi, «[L]le riprese videofilmate costituiscono prove documentali non disciplinate dalla legge, previste dall'art. 189 c.p.p. e pertanto non possono considerarsi assimilabili al "*genus*" delle intercettazioni di conversazioni e comunicazioni. Ne discende che ad esse non si applica la disciplina prevista dagli artt. 266 ss., fermo restando il limite della tutela della libertà domiciliare di cui all'art. 14 Cost., che va valutato di volta in volta». Cfr. sez. V, 7 maggio 2004, n. 24715, in *Arch. nuova proc pen*., 2005, n. 2, p. 526 ss. Sul tema, *amplius*, C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007, p. 253 ss.

[21] Così C. MARINELLI, *Intercettazioni processuali*, cit., p. 66.

[22] C. CARUSO, *La libertà e la segretezza*, cit., p. 6. Secondo tale concezione, accolta dalla dottrina maggioritaria, «[…] il concetto di comunicazioni costituzionalmente tutelate va limitato solo a quelle eseguite per telefono o per iscritto attraverso la corrispondenza epistolare, nonché quelle avvenute attraverso le nuove forme di comunicazione, come i messaggi di posta elettronica, le comunicazioni scambiate in chat e le videoconferenze […]». Così A. DIDDI, *L'inviolabilità della segretezza delle comunicazioni*, cit., p. 269.

[23] L'espressione appartiene a I. CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione ed utilizzazione delle prove c.d. incostituzionali,* in *Giur. it.,* 1999, n. 2, p. 1693.

[24] Propendono per un'interpretazione più ampia della nozione, A. CAMON, *Le intercettazioni*, cit., p. 28 ss.; I. CALAMANDREI, *Acquisizione dei dati esteriori di una comunicazione,* cit., p. 1699; L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 25; ID., *Il rilevamento del "tracciato* axe": *una nuova denominazione per una vecchia tecnologia di indagine*, in *Giur. it*., 1999, n. 2, p. 1687; G. MELILLO, *L'acquisizione dei tabulati*, cit., p. 476 ss.

[25] Cfr. A. DIDDI, *Tutela della* privacy *e acquisizione dei tabulati telefonici*, in *Giust. pen*., 1999, n. 3, p. 628 ss.; A. PACE, *Problematica delle libertà costituzionali,* cit., p. 251; ID*., Nuove frontiere della libertà di 'comunicare riservatamente' (o, piuttosto del diritto alla riservatezza)?,* cit., p. 752 s.; A. ZACCARINI, *Libertà e segretezza della corrispondenza*, in *Riv. pen*., 1995, p. 451. Nello stesso senso anche F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 68 s., il quale esclude dalla sfera di operatività dell'art. 15 Cost. i dati esteriori della comunicazione e ritiene che l'interesse al segreto sul fatto–comunicazione sia solo un particolare aspetto della riservatezza. Più di recente, C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, cit., p. 11, secondo cui «sarebbe forse eccessivo ritenere che tutti i dati esteriori siano elementi inscindibili dalle

momento che i dati esterni alle comunicazioni non rientrano, *tout court*, nel concetto di comunicazione vera e propria[26].

In ragione delle evidenti ripercussioni pragmatiche dell'assunto, la Corte costituzionale interviene a più riprese per chiarire la portata del precetto: aderendo ad un'interpretazione maggiormente elastica della nozione *de qua*, la Consulta ritiene che «[…] la copertura costituzionale è tale da ricomprenderne fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica […]. Cosicché, in mancanza delle garanzie *ivi* previste, il precetto preclude la divulgazione o, comunque, la conoscibilità da parte di terzi delle informazioni e delle notizie idonee a identificare i dati esteriori della conversazione telefonica (autori della comunicazione, tempo e luogo della stessa), dal momento che, facendone oggetto di uno specifico diritto costituzionale alla tutela della sfera privata attinente alla libertà e alla segretezza della comunicazione, ne affida la diffusione, in via di principio, all'esclusiva disponibilità dei soggetti interessati»[27].

---

comunicazioni riservate. Le garanzie richieste dall'art. 15 Cost. (riserva di legge e soprattutto di giurisdizione) andranno applicate solo a quei dati esteriori che, oltre ad essere necessari per l'attuazione del momento comunicativo, possano essere considerati connessi al messaggio, avuto riguardo sia all'intenzione dei soggetti del rapporto, sia all'obiettiva idoneità tecnica del mezzo utilizzato».

[26] Secondo la dottrina la comunicazione si caratterizza per il contributo psicologico del mittente, ossia l'*animus* di esprimere un pensiero nei confronti di un soggetto determinato. Cfr. F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 148 ss.; S. MAINARDI, sub *art. 15 Cost.,* in *Commentario breve alla Costituzione*, a cura di R. Bin-S. Bartole, Cedam, 2008, p. 122 ss. Seguendo tale concezione, si finisce per ritenere che «non costituirà corrispondenza o comunicazione un qualsiasi scritto, anche se redatto in forma epistolare, destinato a rimanere come appunto, nota, diario personale: esso diverrà corrispondenza soltanto quando il soggetto che lo ha redatto maturi l'intenzione di farlo pervenire ad un altro soggetto». P. BARILE–E. CHELI, voce *Corrispondenza (libertà di),* cit., p. 745. I dubbi vengono incrementati anche dalle pronunce della giurisprudenza di legittimità e di quella costituzionale che talvolta ricomprendono l'acquisizione dei tabulati e dei dati esterni alle comunicazioni nel *genus* delle intercettazioni. Cfr. Cass., sez. un., 24 settembre 1998, n. 21, in *Cass. pen*., 1992, n. 2, p. 476 ss. In altri casi, si sottolinea l'incompatibilità tra le due discipline. Cfr. sez. II, 7 ottobre 1998, n. 8248, in *Giur. it.,* 1999, n. 2, p. 1687; sez. un., 8 maggio 2000, n. 6, in *Cass. pen.,* 2000, n. 11, p. 3235; sez. un., 30 giugno 2000, n. 16, in *C.E.D. Cass.,* n. 216247; sez. II, 13 febbraio 2013, n. 21644, *ivi,* n. 255542. Nello stesso senso anche la giurisprudenza della Consulta: Corte cost., 11 marzo 1993, n. 81, in *Cass. pen*, 1993, p. 2741, n. 1640; 17 luglio 1998, n. 281, in *www.giur.cost.it*. Per una puntuale ricostruzione delle disomogenee pronunce sul tema *de qua*, M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont*., 2016, n. 3, p. 157 ss.

[27] Così Corte cost., 6 aprile 1993, n. 81, in *Giur. cost*., 1993, n. 1, p. 731, con nota di A. PACE, *Nuove frontiere della libertà di "comunicare riservatamente" (o, piuttosto, del diritto alla riservatezza?),* cit., p. 744 ss.; in *Cass. pen.,* 1993, n. 10, p. 2746 ss., con nota di D. POTETTI, *Corte costituzionale 81/1993: la forza espansiva della tutela accordata dall'art. 15, c. 1, della Costituzione*. In argomento anche G. DI CHIARA–S. GIANBRUNO, *Temi di giurisprudenza sul processo penale,* Giappichelli, 1999, p. 41 ss.; S. DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali*, in *Giur. it*., 1995, n. 1, p. 107 ss. In senso conforme, Corte cost., 17 luglio 1998, n. 281, in *Giust. pen*., 1998, n. 2, p. 354; 6 novembre 2006, n. 372, in *www.giurcost.org*. Invero la *quaestio de qua* è già stata affrontata dalla Corte europea dei diritti dell'uomo che, discutendo nel 1984 della legittimità della registrazione dei dati esteriori alla comunicazioni, sancisce che «i verbali delle registrazioni contengono informazioni, in particolare i numeri chiamati, quali costituiscono elemento integrante della comunicazione telefonica […] e, dunque, la consegna di queste informazioni alla polizia […] si risolve in un'interferenza con il diritto garantito dall'art. 8 CEDU». Corte EDU, Grande Camera, 2 agosto 1984, *Malone c. Regno Unito*, cit.

Più di recente, la Corte estende ancora maggiormente l'ambito applicativo del dettato costituzionale, accordando la medesima tutela anche al tracciamento delle comunicazioni[28], precisando che «i tabulati delle conversazioni telefoniche consentono di apprendere e individuare tutti i contatti con altre utenze e la loro collocazione temporale, e, nel caso di telefonia mobile, potrebbero anche permettere di effettuare il cosiddetto "tracciamento", vale a dire le localizzazioni e gli spostamenti dei soggetti detentori del terminale telefonico».

A prescindere dall'inclusione di tutti i dati esterni alle comunicazioni nella sfera di tutela di cui all'art. 15 Cost., più genericamente si può affermare che «l'indeterminatezza della formula consente di includervi ogni atto sottratto alla conoscibilità di terzi in quanto volto a trasmettere contenuti comunicativi solo ad uno o più destinatari determinati, rafforza[ndo] l'oggetto della tutela e confer[endo] carattere elastico alla norma»[29], destinata, per questo, a durare nel tempo e ad «adattarsi agli sviluppi della tecnica e riuscire a comprendere nuove possibili forme espressive, inimmaginabili all'epoca della redazione del testo»[30].

Una volta delimitato l'oggetto e il contenuto della tutela, il precetto prosegue introducendo delle deroghe all'inviolabilità dei diritti di libertà e segretezza delle comunicazioni, ovvero i "casi" per cui una loro limitazione è da considerarsi lecita e legittima.

Come giustamente osservato, più che di una deroga si tratta «di un articolato complesso di garanzie»[31] introdotto al fine di delimitare le ipotesi di ingiustificate compressioni[32]: più precisamente, si ritiene che l'ingerenza al diritto di libertà e segretezza possa essere ammessa solo in presenza di due condizioni complementari e non alternative.

In primis, si richiede la sussistenza di provvedimento giurisdizionale corredato di congrua motivazione[33], costituendo la stessa «il livello minimo di garanzia prefigurato dal citato precetto

---

[28] Corte cost., 26 maggio 2010, n. 188, in *www.giurcost.it*. Per commenti, si rinvia a P. COSTANZO, *Le intercettazioni delle comunicazioni interpersonali (un* vademecum *costituzionale),* in *www.consultaonline,* 2016, n. 2, p. 231 ss.; D. PICCIONE, *Utilizzazione di tabulati telefonici nei confronti dei componenti delle Camere e potere di giudicare la "decisività" del mezzo di ricerca della prova per lo svolgimento delle indagini*, in *Giur. cost*., 2010, n. 3, p. 2236 ss.

[29] Così C. PANNACCIULLI, *Profili costituzionali delle intercettazioni di comunicazioni e discrezionalità del giudice*, in *Riv. AIC*, 2012, n. 3, p. 10.

[30] Si esprime così A. VALASTRO, *L'art. 15 e i principi costituzionali,* cit., p. 114.

[31] C. MARINELLI, *Intercettazioni processuali*, cit., p. 68.

[32] Come giustamente osservato, «[…] nello Stato legale ogni limitazione dell'autonomia individuale può avvenire soltanto in forza della legge [mentre] in uno Stato di diritto in senso proprio, alla garanzia della natura dell'atto limitativo […] se ne aggiunge un'altra, espressa nel principio che gli atti della pubblica autorità devono essere sottoposti al sindacato del giudice, affinchè sia assicurata la loro effettiva conformità agli imperativi della legge». Così C. MORTATI, *Le forme di Governo. Lezioni*, Cedam, 1973, p. 39 s.

[33] Con riferimento alle intercettazioni, si è affermato che «la motivazione è posta a tutela del diritto alla segretezza delle conversazioni e comunicazioni e pertanto deve essere alla base del decreto di autorizzazione, di proroga o convalida […] così come quello che non accoglie la richiesta del p.m.» (L. FILIPPI, sub *art. 267*, in *Codice di procedura penale commentato*, V ed., cit., p. 2628), la giurisprudenza di legittimità ha determinato il contenuto "minimo" della motivazione del provvedimento, per cui «[…] l'obbligo motivazionale non può ritenersi assolto con il ricorso a citazioni o perifrasi apodittiche del contenuto delle norme che disciplinano l'assunzione del mezzo probatorio, né con il mero richiamo alle richieste degli organi investigativi. […] Il giudice deve fornire concreta dimostrazione del corretto uso del potere conferitogli tramite un'adeguata e specifica motivazione del provvedimento autorizzativo». Così Cass., sez. VI, 25 novembre 2003, n. 727, in *C.E.D. Cass.,* n. 227895. In dottrina, *ex plurimis*, V. CAMPILONGO, *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi,* in *Cass. pen*., 2005, f. 10, p. 3196 ss. Tuttavia, come affermato dalla Corte europea dei diritti dell'uomo, «non sussiste violazione dell'art. 8 CEDU nel caso in cui il g.i.p. abbia autorizzato l'esecuzione di intercettazioni ambientali mediante un provvedimento motivato per *relationem*». Corte EDU, sez. II, 10 aprile 2007,

costituzionale per la limitazione del diritto in questione, allo scopo di assicurare un equo contemperamento fra il diritto stesso e l'interesse alla prevenzione e alla repressione dei reati, oggetto anch'esso di protezione costituzionale»[34] (riserva di giurisdizione)[35].

Panarisi c. Italia, cit. Nello stesso senso già, Cass., sez. un., 26 febbraio 1991, n. 5, in *Cass. pen.,* 1991, n. 2, p. 490 ss. Anche in questa ipotesi è opportuno che «si possa dedurre l'*iter* cognitivo e valutativo seguito dal giudice e se ne possano conoscere i risultati che debbono essere conformi alle prescrizioni di legge». Cass. sez. un., 21 giugno 2000, n. 17, in *Cass. pen*., 2001, n. 1, p. 69 ss. Nello stesso senso, da ultimo, sez. un., 27 luglio 2018, n. 36072, in *Cass. pen.,* 2018, f. 12, p. 4088 ss. secondo cui «il decreto di sequestro probatorio, così come l'eventuale decreto di convalida, anche qualora abbia ad oggetto cose costituenti corpo di reato, deve contenere una specifica motivazione in ordine alla finalità perseguita per l'accertamento dei fatti». Per un commento, v. G. SCHENA, *Quello che le Sezioni unite non dicono a proposito di "idoneità della motivazione" nel caso di sequestro probatorio del* corpus delicti, in *Cass. pen.,* 2018, f. 12, p. 4088 ss.

[34] Corte cost., 30 novembre 2009, n. 320, in *Giur. cost*., 2009, f. 3, p. 4823, con nota di M. VILLANI, *La Corte ribadisce i rapporti tra legalità costituzionale, legalità sostanziale e legalità processuale.*

[35] Sul carattere assoluto della riserva di giurisdizione, V. ANGIOLINI, *Riserva di giurisdizione e libertà costituzionali*, Cedam, 1967; G. BASCHIERI–L. BIANCHI D'ESPINOSA–C. GIANNATTASIO, *La Costituzione italiana*, Niccoli, 1949, p. 89 s.; C. CHIOLA, *Vie nuove all'intercettazione delle comunicazioni*, in *Dir. e soc.,* 1979, p. 133; V. ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni,* cit., p. 132; V. MATTERA, *La recente disciplina delle intercettazioni telefoniche nel quadro dei precedenti legislativi*, in *Riv. polizia,* 1979, p. 392 ss.; G. MOFFA, *Libertà delle comunicazioni e intercettazioni telefoniche*, in *Giust. pen.,* 1971, p. 257 ss.; A. ZACCARINI, *Libertà e segretezza della corrispondenza*, cit., p. 447.

In secondo luogo, è indispensabile la presenza una norma giuridica che legittimi la l'ingerenza[36] (riserva di legge)[37], al fine di contenere il potere discrezionale del magistrato e, al contempo, scongiurare il rischio di eventuali abusi da parte degli organi inquirenti[38].

Conclusa la disamina inerente alla normativa nazionale, va detto che la libertà e la segretezza della corrispondenza e delle comunicazioni trova ampio riscontro anche nel diritto internazionale pattizio, «in quanto la disciplina convenzionale ha da tempo assunto il compito di promuovere e proclamare il rispetto dei diritti umani»[39].

[36] La dottrina, attraverso il raffronto tra il disposto degli artt. 15, comma 2 e 13 Cost., ritiene che la prima norma predisponga una tutela maggiormente assorbente del diritto di libertà. L'espressione utilizzata dall'art. 15 Cost., infatti, nel riferirsi alle garanzie stabilite dalla legge sembra alludere ad un *quid pluris* rispetto alla mera predeterminazione dei casi e dei modi nei quali si ammette la compressione del valore tutelato. In questo senso P. BARILE–E. CHELI, voce *Corrispondenza (libertà di),* cit., p. 740; P. BRUNO, voce *Intercettazioni di comunicazioni o conversazioni*, cit., p. 188; A. CAMON, *Le intercettazioni nel procedimento penale*, cit., p. 108; F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 61; C. CARUSO, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, cit., p. 8 s.; G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 59 s.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 69.

[37] Sul carattere di assolutezza della riserva di legge, da ultimo, Corte cost., 24 gennaio 2017, n. 20, in *Dir. pen. cont.,* 15 marzo 2017, con nota di E. ANDOLFATTO, *Il nuovo giudizio di legittimità costituzionale sulla sospensione del procedimento con messa alla prova: la consulta respinge tre questioni sollevate dal tribunale di Prato*. In dottrina, senza pretesa di completezza e limitandosi ad alcuni recenti lavori, AA. VV., *Il diritto penale nella giurisprudenza costituzionale*, a cura di E. D'orlando–L. Montanari, Wolters Kluwer, 2009; M.A. CABIDDU–P. DAVIGO, *Leggi penali di favore ed efficacia «*in malam partem*» delle sentenze della Corte costituzionale*, in AA. VV., *«Effettività» e «seguito» delle tecniche decisorie della Corte costituzionale*, a cura di R. Bin–G. Brunelli–A. Pugiotto–P. Veronesi, ESI, 2006, p. 255 ss.; C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* cit., p. 1216 ss.; M. D'AMICO, *Corte costituzionale e discrezionalità del legislatore in materia penale*, in *Riv. AIC*, f. 4, 17 novembre 2016; ID., *Il principio di legalità in materia penale fra Corte costituzionale e Corti europee*, in AA. VV., *Le Corti dell'integrazione europea e la Corte costituzionale italiana*, a cura di N. Zanon, ESI, 2006, p. 167 ss.; L. FILIPPI, voce *Intercettazioni telefoniche (dir. pen. proc.),* in *Enc. dir.,* Agg. VI, Giuffrè, 2002, p. 572 s.; A. LOLLO, *Norme penali di favore e zone d'ombra della giustizia costituzionale*, in *www.federalismi.it*, f. 13, 29 giugno 2009; I. PELLIZZONE, *Profili costituzionali della riserva di legge in materia penale. Problemi e prospettive*, Franco Angeli, 2016; M. SCOLETTA, *Metamorfosi della legalità*. Favor libertatis *e sindacabilità* in malam partem *delle norme penali*, Monboso, 2012; N. ZANON, *Corte costituzionale e norme penali di favore: verso un sindacato sulle scelte politico–criminali?*, in AA. VV., *Verso un sindacato di legittimità sulle scelte politico–criminali?*, a cura di L. Zilletti–F. Oliva, ETS, 2007, p. 53 ss.

[38] In tema, diffusamente, A. SPERTI, *La libertà e segretezza della corrispondenza e delle comunicazioni tra vecchie e nuove prospettive di tutela dci diritti fondamentali*, in AA. VV., *Il rispetto delle regole. Scritti degli allievi in onore di Alessandro Pizzorusso,* Giappichelli, 2005, p. 21.

[39] Si esprimono così V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, Il Mulino, 2016, p. 17. Nello stesso senso, E. MALFATTI, *I "livelli" di tutela dei diritti fondamentali nella dimensione europea,* Giappichelli, 2018, p. 99 ss.

Il riferimento va innanzitutto all'art. 8 CEDU che, tra gli altri diritti tutelati[40], garantisce il rispetto della corrispondenza[41], qui intesa come «ogni forma di comunicazione privata da persona a persona»[42], escludendo l'ingerenza da parte della pubblica autorità al godimento dei diritti *ivi* menzionati, a meno che la stessa non risponda alle condizioni esposte nella clausola di limitazione di cui al comma 2[43].

La prima condizione impone che qualsiasi interferenza statale nel godimento del diritto, perché sia considerata legittima, deve essere prevista dalla legge nazionale, intendendo come tale «la norma in vigore nel sistema nazionale, così come interpretata dai tribunali»[44].

---

[40] L'art. 8 CEDU, al comma 1, riconosce ad ogni persona il diritto al rispetto della sua vita privata e familiare (c.d. diritto alla riservatezza) nonché del domicilio. Preme sottolineare che il precetto *de qua* è quello che su cui, nel corso del tempo, si è maggiormente concentrata la giurisprudenza evolutiva della Corte europea: anche se la stessa ha più volte ribadito che non possono essere riconosciuti tutti i diritti di ultima generazione non contemplati dalla Convenzione, la stessa amplia progressivamente l'ambito di tutela del diritto in esame. Cfr. Corte EDU, Grande Camera, 12 settembre 2012, *Nada c. Svizzera*, n. 10593/08, §§ 151–154; sez. I, 14 ottobre 2010, *A. c. Croazia*, n. 55164/08, § 55–61; sez. II, 24 febbraio 2009, *Errico c. Italia*, n. 29768/05, § 54–62; sez. I, 5 marzo 2009, *Sandra Jankovic c. Croazia*, n. 38478/05, § 45–59; Grande Camera, 30 novembre 2004, *Oneryildiz c. Turchia*, n. 48939/99, §160; Grande Camera, 22 febbraio 1994, *Burghartz c. Svizzera*, n. 16213/90, § 24; Grande Camera, 9 dicembre 1994, *Lopez Ostra c. Spagna*, n. 16798/90, § 58.

[41] Per una puntuale disamina della libertà di corrispondenza così come tutelata dall'art. 8 CEDU, *ex multis,* M. BONETTI–A. GALLUCCIO, sub *art. 8 CEDU. Profili specifici*, in AA. VV., *Corte di Strasburgo e giustizia penale*, cit., p. 264 ss.; G. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, cit., p. 44 ss.; L. TOMASI, sub *art. 8*, in AA. VV., *Commentario breve alla Convenzione europea dei diritti dell'uomo*, a cura di S. Bartole–P. De Sena–V. Zagrebelsky, Cedam, 2012, p. 123 ss.; V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 23 ss.

[42] Così V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 227. La precisazione, in questo caso, appare doverosa dal momento che se si trattasse di una comunicazione diretta alla generalità del pubblico ricadrebbe nell'ambito di protezione dell'art. 10 CEDU, in quanto forma di espressione.

[43] Sul punto si veda, *amplius*, A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, in AA. VV., *I principi europei del processo penale*, cit., p. 363 ss. Cfr. anche A. GALLUCCIO, sub *art. 8 Cedu. Profili generali sugli artt. 8–11 CEDU*, cit., p. 256 ss.

[44] Così V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 127. Nello stesso senso, M. BONETTI–A. GALLUCCIO, sub *art. 8 CEDU. Profili specifici*, in AA. VV., *Corte di Strasburgo e giustizia penale*, cit., p. 264; A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, cit., p. 374 ss. La Corte europea, a differenza di quanto accade nell'ordinamento nazionale per cui il significato di "legge" è da attribuirsi in senso assoluto, con esclusione di ogni fonte subordinata, adotta una nozione sostanziale e non formale di "diritto", non essendo assolutamente rilevante l'origine parlamentare della norma. Nella nozione convenzionale, infatti, è compresa ogni norma giuridica, qualunque sia l'origine e la posizione nella gerarchia delle fonti. Sul punto la giurisprudenza è cospicua. *Ex plurimis,* Corte EDU, Grande Camera, 10 novembre 2005, *Leyla Sahin c. Turchia*, n. 44774/98, § 88; sez. II, 21 giugno 2005, *Perincek c. Svizzera*, n. 46669/99, § 131–136; sez. II, 2 agosto 2001, *N. F. c. Italia*, n. 37119/97, §§18–19 e 31. Ma già Grande Camera, 25 marzo 1985, *Barthold c. Germania,* n. 8734/79, §46. Inoltre, rientra nella nozione di legge anche quella non scritta formulata dalla giurisprudenza dal momento che una diversa interpretazione priverebbe della tutela derivante dalla Convenzione gli Stati il cui sistema normativo si fonda sulla *common law*, sul presupposto che «si sbaglierebbe a forzare la differenza tra i Paesi di *common law* e quelli continentali; la legge scritta è importante naturalmente per i primi. Viceversa, la giurisprudenza gioca tradizionalmente un ruolo considerevole nei secondi, al punto tale che settori interi del diritto positivo sono il risultato, in larga misura, delle decisioni delle Corti e dei tribunali». Così Corte EDU, Grande Camera, 24 aprile 1990, *Kruslin c. Francia*, n. 11801/85, § 29. Nello stesso senso, Grande Camera, 25 febbraio 1993, *Funke c. Francia*, n. 10828/84, § 49; Grande Camera, 25 febbraio 1993, *Cremieux c. Francia*, n. 11471/85. Ma già Grande Camera, 26 aprile 1979, *Sunday*

In secondo luogo, l'ingerenza deve palesarsi come necessaria in una società democratica[45] per la sicurezza nazionale[46], per la sicurezza pubblica[47], per il benessere economico del Paese[48], per la difesa dell'ordine e per la prevenzione dei reati[49], per la protezione della salute o della morale[50] o anche per protezione dei diritti e delle libertà degli altri individui[51].

Va detto che la Convenzione, a differenza del diritto italiano, non richiede che l'interferenza sia sottoposta alla riserva di giurisdizione, ossia all'autorizzazione motivata dell'autorità giudiziaria. Tuttavia, la mancanza viene giustificata dalla dottrina dominante[52] in ragione della

---

Times c. Regno Unito, cit., § 47. Più di recente, sez. III, 15 febbraio 2011, *Geleri c. Romania*, n. 33118/05, § 30.

[45] Circa la nozione di "necessità", la CEDU chiarisce che tale requisito non va inteso in termini di assoluta indispensabilità dell'interferenza ma piuttosto di una sua auspicabilità. V., Corte EDU, 24 ottobre 1983, *Silver e altri c. Regno Unito*, cit., p. 73, secondo cui «il predicato "necessario" non è sinonimo di "indispensabile", né possiede la flessibilità di termini come "ammissibile", "normale", "utile", "ragionevole", "opportuno"». Nello stesso senso, anche Grande Camera, 7 dicembre 1976, *Handyside c. Regno Unito*, n. 5493/72, § 48. Necessaria, secondo la giurisprudenza della Corte, è una limitazione del diritto protetto che corrisponda ad un pressante bisogno sociale e che sia proporzionata rispetto alla finalità legittima perseguita. In questo senso Corte EDU, Grande Camera, 24 marzo 1988, *Olsson c. Svezia*, n. 10465/83; sez. V, 6 gennaio 2011, *Pakas c. Lituania*, n. 34932/04, § 100, per cui ogni ingerenza alla vita privata è ammessa se compatibile con le esigenze della democrazia e dello stato di diritto. In dottrina, esaustivamente, A. GALLUCCIO, sub *art. 8 Cedu. Profili generali sugli artt. 8–11 CEDU*, cit., p. 259 s.

[46] La nozione si presenta unitamente allo scopo di salvaguardare la sicurezza pubblica e l'ordine e prevenire la commissione dei reati. In questo senso V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 132. In giurisprudenza, Corte EDU, Grande Camera, 6 novembre 1978*, Klass e altri c. Germania*, n. 5029/71, in *Foro it*., 1979, p. 1; Grande Camera, 2 agosto 1984, *Malone c. Regno Unito*, cit.

[47] La nozione rinvia a uno scopo legittimo spesso considerato dalla Corte insieme ad altri, come quello della protezione della salute pubblica o dei diritti altrui. Cfr. Corte EDU, sez. I, 25 settembre 1996, *Buckley c. Regno Unito*, n. 20348/92, §§ 62–63.

[48] Il benessere economico del Paese è spesso ricompreso nella nozione di interesse pubblico. V. Corte EDU, Grande Camera, 8 luglio 2003, *Hatton e altri c. Regno Unito*, n. 36022/97, §§ 121 e 126–129; sez. III, 22 dicembre 2015, *G.S.B. c. Svizzera*, n. 28601/ 11, § 83.

[49] La Corte adotta una nozione assai restrittiva del concetto di "ordine pubblico", assimilandolo alla sicurezza e alla prevenzione di disordini sociali. Cfr. sul punto, Corte EDU, sez. II, 9 luglio 2013, *Vona c. Ungheria*, n. 35943/10, § 52; sez. II, 7 ottobre 2008, *Eva Molnar c. Ungheria*, n. 10346/05, § 43; sez. II, 9 febbraio 2002, *Cisse c. Francia*, n. 51346/99, §§ 44–46; 21 giugno 2005, *Perincek c. Svizzera*, n. 46669/99, §§ 145–151.

[50] In relazione all'esigenza di protezione della salute, la Corte ammette limitazioni al diritto di cui all'art. 8 CEDU, sia in relazione a quella della singola persona fisica (come nei trattamenti sanitari obbligatori e nell'imposizione di vaccinazioni), sia a quella generale (ad esempio, nell'imposizione di test alcolici a conduttori di veicoli). Cfr. Corte EDU, sez. III, 19 ottobre 2010, *Scozzari e altri c. Italia*, n. 67790/01. In relazione, invece, alla difesa della morale, la Corte riconosce che non esiste un "sentire comune" in materia di moralità ma che esistono posizioni assai diversificate, accordando un ampio margine di apprezzamento sulla necessità di interferenza nel diritto dell'individuo. In questo senso Corte EDU, sez. III, 16 febbraio 2010, *Akdas c. Turchia*, n. 41056/04. V., altresì, Grande Camera, 7 dicembre 1976, *Handyside c. Regno Unito*, cit., § 46.

[51] V. Corte EDU, Grande Camera, 20 settembre 1994, *Otto–Preminger–Institut c. Austria*, n. 13470/87, § 48; Grande Camera, 25 marzo 1985, *Barthold c. Germania*, cit. §§ 50–51. Secondo la giurisprudenza europea le limitazioni ai diritti devono considerarsi come tassative e interpretate in senso restrittivo. In questo senso Corte EDU, sez. I, 12 febbraio 2009, *Nolan e K. c. Russia*, n. 2512/04, § 73; Grande Camera, 10 dicembre 2007, *Stoll c. Svizzera*, n. 69698/01, §§54–56. *Contra* Grande Camera, 1 luglio 2014, *S.A.S. c. Francia*, n. 43835/11, § 113

[52] In questo senso P. BALDUCCI, *Le garanzie nelle intercettazioni tra costituzione e legge ordinaria*, cit., p. 202; A. BALSAMO–A. TAMIETTI, *Le intercettazioni tra garanzie formali e sostanziali*, cit., p. 425

severità dei controlli della giurisprudenza europea sulla sussistenza del principio di proporzione dell'interferenza[53] che consente di soddisfare il criterio della necessità democratica: per poter essere ritenuta legittima, dunque, la compressione deve essere «proporzionata rispetto alla giustificazione invocata al fine di non oltrepassare i limiti della stretta necessità»[54].

Parallelamente alla tutela accordata dall'art. 8 CEDU, il diritto alla corrispondenza trova autonoma protezione anche in altre fonti convenzionali.

In particolare, nell'art. 17 del Patto sui diritti civili e politici del 1948[55], ai sensi del quale «[N]nessuno può essere sottoposto ad interferenze arbitrarie o illegittime […] nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione», nonché nell'art. 7 della Carta dei diritti fondamentali dell'UE[56], per cui «[O]gni individuo ha diritto al rispetto […]

ss.; A. BARGI–S. FURFARO, *Le intercettazioni di conversazioni e comunicazioni,* in AA. VV., *La prova penale*, a cura di A. Gaito, Utet, 2008, p. 119 ss.; L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 43; S. FURFARO, *Un problema irrisolto: le intercettazioni telefoniche*, in AA. VV., *Procedura penale e garanzie europee,* cit., p. 122; A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, cit., p. 381. *Contra* G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 8, il quale ritiene che le garanzie apprestate dall'art. 15 Cost., nonostante l'indeterminatezza, siano più rigorose di quelle ricavabili dalla Convenzione.

[53] Il *test* di proporzionalità della misura rappresenta il cuore dell'esame della giustificazione dell'ingerenza statale nei diritti fondamentali. Esso rappresenta una fondamentale inversione dei rapporti tra la persona e l'autorità: in questo caso sono le pubbliche autorità che, per legittimare le proprie azioni od omissioni, devono dimostrare che le scelte adottate non incidono in maniera sproporzionata sui diritti delle persone. Sul principio di proporzione quale canone di legittimità della misura intrusiva adottata, così come introdotto dalla giurisprudenza creativa della giurisprudenza europea, v. Corte EDU, sez. I, 20 settembre 2018, *Solka e Rybicka c. Polonia*, n. 30491/17, in cui la Corte ravvisa uno squilibrio tra le esigenze investigative e il diritto al rispetto della vita privata e familiare, dal momento che non sono stati presi in considerazioni mezzi di indagine meno invasivi rispetto agli esami autoptici; inoltre, la legislazione interna non prevede rimedi giurisdizionali volti a sindacare l'arbitrarietà della decisione del pubblico ministero.

[54] Così Corte EDU, sez. III, 14 marzo 2002, *Puzinas c. Lituania*, n. 44800/98; sez. I, 9 gennaio 2001, *Natoli c. Italia*, n. 26161/95, § 33; 23 settembre 1998, *McLeod c. Regno Unito*, 24755/94, § 53.

[55] La Convenzione Internazionale sui Diritti Civili e Politici è un Trattato delle Nazioni Unite, adottato nel 1966 ed entrato in vigore il 23 marzo del 1976 e reso esecutivo con la legge 25 ottobre 1977, n. 881, recante "*Ratifica ed esecuzione del patto internazionale relativo ai diritti economici, sociali e culturali, nonché del patto internazionale relativo ai diritti civili e politici, con protocollo facoltativo, adottati e aperti alla firma a New York rispettivamente il 16 e il 19 dicembre 1966*", in *Gazz. uff.,* 7 dicembre 1977, n. 333, in *www.gazzettaufficiale.it*.

[56] La Carta dei diritti fondamentali dell'Unione europea (2000/C 364/01), nota come Carta di Nizza, è stata solennemente proclamata a Nizza il 7 dicembre 2000. *Ex multis*, AA. VV., *L'Europa dei diritti,* a cura di R. Bifulco–M. Cartabia–A. Celotto, Il Mulino, 2001, *passim*; A. LOIODICE, *Centralità della persona umana nella Carta di Nizza e nella Convenzione Europea,* in AA. VV., *Verso una Costituzione europea*, a cura di L. Leuzzi–C. Mirabelli, Marco editore, 2003, p. 427 ss. Con l'entrata in vigore del Trattato di Lisbona (1 dicembre 2009), assume il medesimo valore giuridico dei Trattati e si pone dunque come pienamente vincolante per le istituzioni europee e gli Stati membri e, allo stesso livello di trattati e protocolli ad essi allegati, come vertice dell'ordinamento dell'Unione europea. Cfr. AA. VV., *Diritti fondamentali e politiche dell'Unione europea dopo Lisbona*, a cura di S. Matteucci–F. Guarriello–P. Puoti, Maggioli editore, 2013. Più di recente, N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. Limiti di applicazione*, Franco Angeli, 2018; R. MASTROIANNI–S. ALLEGREZZA–O. POLLICINO, *Carta dei diritti fondamentali dell'Unione europea*, Giuffrè, 2017.

delle sue comunicazioni»[57], che per effetto della c.d. clausola di adeguamento del diritto interno a quello internazionale, assumono valore vincolante nell'ordinamento giuridico nazionale[58].

[57] Come rilevato, la formulazione letterale dell'art. 7 Carta UE è assolutamente identica a quella dell'art. 8 CEDU, tranne che per la sostituzione del termine "corrispondenza" con quello più moderno di "comunicazione". I diritti garantiti hanno la stessa portata dei corrispondenti diritti della Convenzione, salva la possibilità che il diritto dell'Unione assicuri una protezione più estesa (art. 52 comma 3 Carta UE). Sul punto, V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 245 s.

[58] L'adesione dell'Italia ai Trattati convenzionali e internazionali determina l'automatico ingresso della disciplina *ivi* contenuta nell'ordinamento nazionale attraverso la c.d. clausola di adeguamento di cui all'art. 11 Cost. In tema S. CASSESE, *L'efficacia delle norme italiane di adattamento alla Convenzione europea dei diritti dell'uomo,* in *Riv. dir. int. priv. proc*., 1969, p. 918 ss.; M. CHIAVARIO, *Cultura italiana del processo penale e Convenzione europea dei diritti dell'uomo: frammenti di appunti e spunti per una microstoria*, in *Riv. internaz. dir. uomo*, 1990, p. 433; ID., *La convenzione europea dei diritti dell'uomo nel sistema delle fonti normative in materia penale*, Giuffrè, 1969, p. 19 ss.; G. RAIMONDI, *La Convenzione europea dei diritti dell'uomo nella gerarchia delle fonti dell'ordinamento italiano*, in *Riv. internaz. dir. uomo*, 1990, p. 36 ss. Con specifico riferimento alla CEDU, assai interessante è la questione legata all'efficacia della stessa nell'ordinamento interno. Nelle c.d. "sentenze gemelle" del 2007 si è affermato che il novellato art. 117 comma 1 Cost. posiziona le norme CEDU ad un livello gerarchico interposto tra la legge ordinaria e la Costituzione. Si è escluso, per converso, che le disposizioni della stessa Convenzione possano avere diretta applicazione nell'ordinamento interno in forza dell'art. 11 Cost. e che il giudice nazionale possa disapplicare la normativa interna contrastante con essa senza sollevare questione di legittimità costituzionale. Cfr. Corte cost., 22 ottobre 2007, n. 348, in *Giur. it*., 2008, p. 573 ss., con nota di R. CALVANO, *La Corte costituzionale e la CEDU nella sentenza 348/2007*; 22 ottobre 2007, n. 349, *ivi*, p. 205 ss. Successivamente, Corte cost., 13 febbraio 2009, n. 39, in *www.giurcost.org*; 26 novembre 2009, n. 311, *ivi*; 4 dicembre 2009, n. 317, *ivi*; 8 marzo 2010, n. 93, in *Giur. cost*., 2010, p. 1053 ss.; 8 giugno 2011, n. 180, in *www.giurcost.org*; 10 giugno 2011, n. 181, *ivi*; 5 aprile 2012, n. 78, *ivi*. Queste conclusioni sono state messe nuovamente in discussione dalle disposizioni sui diritti fondamentali contenute nell'art. 6 Trattato sull'Unione europea, come riformato dal Trattato di Lisbona (13 dicembre 2007). La Consulta, nel 2011, ha negato l'avvenuta "comunitarizzazione" della Convenzione Europea, contraddicendo in modo aperto alcune decisioni giurisprudenziali e impostazioni dottrinali che avevano ritenuto i principi CEDU direttamente applicabili nel nostro ordinamento, in quanto entrati a far parte di quel sistema di valori comunitari che informano l'intera attività legislativa dell'Unione. Così Corte cost., 11 marzo 2011, n. 80, in *Giur. cost*., 2011, p. 1224 ss. In dottrina, A. CELOTTO, *Il Trattato di Lisbona ha reso la CEDU direttamente applicabile nell'ordinamento italiano?,* in *www.giustamm.it;* G. COLAVITTI–C. PAGOTTO, *Il Consiglio di Stato applica direttamente le norme CEDU grazie al Trattato di Lisbona: l'inizio di un nuovo percorso?,* in *Guida dir.*, 2010, n. 14, p. 88 ss.; L. D'ANGELO, *"Comunitarizzazione" dei vincoli CEDU in virtù del Trattato di Lisbona? No senza una* expressio causae, in *www.forumcostituzionale.it. Contra*, Cons. Stato, sez. IV, 2 marzo 2010, n. 1220, in *Guida dir.*, n. 14, 2010, p. 88 ss., e Tar Lazio, sez. II, 18 maggio 2010, n. 11984, in *Riv. giur. edilizia*, 2010, n. 4, p. 1259. Esse hanno interpretato le previsioni del Trattato di Lisbona nel modo più ampio possibile, riconoscendo a pieno titolo la possibilità di applicare il diritto convenzionale "comunitarizzato" senza il preventivo vaglio di costituzionalità svolto dalla Corte Costituzionale. Anche una parte minoritaria di dottrina propende per la diretta applicazione della Convenzione all'interno degli ordinamenti degli Stati membri. Sul punto, L. DANIELE, *Diritto dell'Unione europea. Sistema istituzionale, ordinamento, tutela giurisdizionale, competenze,* Giuffrè, 2010, p. 220; F. SORRENTINO, *Nuovi profili costituzionali dei rapporti tra diritto internale, internazionale e comunitario*, in *Dir. pubbl. comp. eur*., 2002, p. 1359. In tema, più di recente, R.E. KOSTORIS, *La costruzione dei diritti fondamentali, la Carta di Nizza e le prospettive di adesione dell'Unione alla CEDU*, in AA. VV., *Manuale di procedura penale europea*, cit., p. 78 ss. Per un quadro d'insieme dei rapporti tra diritto interno, CEDU e diritto dell'UE, E. ANDOLINA, *Nuovi scenari nella tutela penale dei diritti fondamentali in Europa*, in *Dir. pen. proc*., 2012, p. 764 ss.; A. GAITO, *Un processo penale verso il modello europeo*, in AA. VV., *Procedura penale e garanzie europee*, cit., p. 1 ss.; R.E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del*

Da quanto detto, emerge che il precetto *de qua* - in tutte le sue declinazioni, sia interne che internazionali- impone di seguire un criterio rigoroso nella ricostruzione del sistema che non ammetta interpretazioni estensive o analogiche: l'aver sottoposto la deroga alla libertà e segretezza delle comunicazioni ad una espressa previsione legislativa si traduce, sul piano fattuale, nell'impossibilità di limitare tale prerogativa in assenza di norme che la contemplino, sul presupposto per cui «ciò che non è espressamente previsto non è consentito»[59].

Si potrebbe, allora, ipotizzare che il silenzio normativo riservato alle innumerevoli potenzialità investigative del *Trojan* debba essere interpretato come un implicito divieto probatorio[60], posto che in materia di libertà e segretezza delle comunicazioni l'art. 15 Cost. impone la "riserva di legge", oltre a quella di "giurisdizione". In chiave di principio, la stessa Corte costituzionale ha non solo affermato che il diritto alla segretezza «non può subire restrizioni e limitazioni da alcuno dei poteri costituiti se non in ragione dell'inderogabile soddisfacimento di un interesse pubblico primario costituzionalmente rilevante»[61] ed in misura «strettamente necessaria alla tutela di quell'interesse»[62] ma ha anche puntualizzato che è in ogni caso necessario che ricorrano «concrete, gravi esigenze di giustizia»[63].

Seguendo un simile ragionamento, solo le attività di intercettazione di conversazioni e comunicazioni tra presenti a mezzo *Trojan* possono ritenersi legittime, in quanto frutto di un'espressa regolamentazione offerta dal *dictum* di cui all'art. 266, commi 2 e 2 *bis* c.p.p. Viceversa, il complesso di investigazioni esperibili mediante il *virus* informatico (al netto delle captazioni *strictu sensu* intese) devono ritenersi illegittime in quanto non contemplate dal dettato legislativo e nemmeno è pensabile che il suo impiego possa essere legittimato in sede giurisprudenziale attraverso interpretazioni estensive in una materia governata da un rigido principio di tassatività [64].

3. L'INVIOLABILITÀ DEL DOMICILIO: IL COMPLESSO ADEGUAMENTO DELLA NOZIONE AL DIRITTO VIVENTE

Le intercettazioni di conversazioni e comunicazioni tra presenti determinano un'ingerenza del diritto all'inviolabilità del domicilio (art. 14 Cost.) in quanto espletabili, ai sensi del comma 2 dell'art. 226 c.p.p., anche nei luoghi di privata dimora di cui all'art. 614 c.p.

---

pluralismo giuridico postmoderno, in *Riv. it. dir. proc. pen*., 2015, p. 1177; V. MANES, *I principi penalistici del* network *multilivello: trapianto, palingenesi,* cross–fertilization, *ivi*, 2012, p. 839 ss.

[59] F. DINACCI, *L'irrilevanza processuale delle registrazioni di conversazioni tra presenti*, in *Giur. it.,* 1994, p. 67.

[60] Come precisato dalla dottrina, «[S]se quindi è vero che alcune forme di impiego del captatore informatico fuoriescono dal perimetro operativo degli artt. 13 e 14 Cost., allora sembra potersi correttamente affermare che sarebbe stato decisamente preferibile un esplicito duplice divieto di acquisizione e di utilizzazione dei risultati ottenuti mediante funzioni investigative diverse dalla captazione sonora». Così L. FILIPPI, *La delega in materia dell'uso del captatore informatico,* in AA. VV., *La riforma Orlando*, a cura di G. Spangher, Pacini Giuridica, 2017, p. 151 ss.

[61] Corte cost., 23 luglio 1991, n. 366, in *Giur. cost.,* 1991, p. 2914 ss.; 24 febbraio 1994, n. 63, in *Giust. pen*., 1994, n. 1, p. 265. In dottrina si veda P. BALDUCCI, *Le garanzie nelle intercettazioni,* cit., p. 49 ss.

[62] Corte cost., 23 luglio 1991, n. 366, cit.

[63] Corte cost., 6 aprile 1973, n. 34, in *Giur. Cost*., 1973, p. 340 ss., con nota di V. GREVI, *Insegnamenti, moniti e silenzi della Corte costituzionale in tema di intercettazioni telefoniche.*

[64] Cfr. AA.VV., *Necessaria una disciplina legislativa in materia di captatori informatici (c.d.* "trojan"): *un appello al legislatore da parte di numerosi docenti di diritto italiani*, in *Dir. pen. cont.*, 7 ottobre 2016.

Prima di soffermarsi sul contenuto del precetto, è indispensabile delineare l'ambito applicativo della prerogativa in questione al fine di scongiurare il rischio di un'ingiustificata sovrapposizione con gli altri diritti della personalità.

Rispetto alla concezione tradizionale[65], la strumentalità della tutela del domicilio al complesso di diritti di libertà sembra essersi fortemente attenuata «finendo il primo per rappresentare un diritto autonomo, in cui si compenetrano diverse esigenze, quali la necessità di garantire, nei luoghi qualificabili come privata dimora, il rispetto del diritto alla libertà personale, il diritto alla libertà e alla segretezza di ogni forma di comunicazione, il diritto alla riservatezza»[66].

L'esigenza di attribuire una connotazione autonoma al precetto *de qua* sembra trovare conferma nell'impostazione prescelta dall'art. 8 CEDU, nonché dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea[67] e dall'art. 12 della Dichiarazione universale dei diritti dell'uomo[68], che, pur delineandolo congiuntamente al diritto al rispetto della vita privata e della corrispondenza, lo qualifica come una «facoltà a sé stante»[69].

Ciò premesso, non è sempre agevole comprenderne l'essenza, e, più in particolare, individuare la corretta declinazione della nozione di "domicilio", assai abusati in ambito interno ed internazionale.

In effetti, né la Carta costituzionale né la CEDU forniscono alcuna definizione di "domicilio", e ciò «al fine di evitare qualunque forma di irrigidimento e cristallizzazione»[70].

---

[65] Come sosteneva G. AMATO, *Commento all'art. 14 Cost.,* cit., p. 54, i diritti in questione risultano complementari e speculari. Infatti, almeno inizialmente, l'inviolabilità del domicilio «esprime la necessità di proteggere la sfera intima della propria casa in connessione con la tutela della proprietà e della sicurezza personale». Nello stesso senso, A. AMORTH, *La Costituzione italiana,* Giuffrè, 1948, p. 62. Nello stesso senso, più di recente, V. COCOZZA, *Percorsi ricostruttivi per la lettura della Costituzione italiana*, Giappichelli, 2014, p. 253 s.

[66] Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 50. Nello stesso senso, C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 74 s. Più di recente M. MONTAGNA, *Libertà domiciliare*, in AA. VV., *Diritti della persona e nuove sfide del processo penale,* cit., p. 119 ss., secondo cui «[N]non si tratta […] esclusivamente del diritto di essere lasciato solo: nel domicilo, un soggetto realizza la propria personalità ed è essa, nelle sue molteplici espressioni, a meritare specifica tutela». D'altra parte, una simile impostazione sembra essere preferita anche dai Padri costituenti. Come sostenuto, «[…] l'art., 14 Cost. sembra essere stato delineato a titolo di sdoppiamento dell'art. 8 (diritto alla libertà personale) e al fine di dare rilievo speciale alla libertà di domicilio, che […] rappresenta cosa talmente sacra e così integrante della persona che non possiamo non garantirlo in modo particolare ed evidente». Così Assemblea costituente (U. Tupini), LXXXII, 10 aprile 1947, p. 2690, cfr. *www.atticamera.it*.

[67] CGUE, 10 settembre 2014, *Monika Kusionovà c. SMART Capital a.s.,* C. 34/13.

[68] Ai sensi dell'art. 12 della Dichiarazione universale dei diritti dell'uomo, «[N]nessuno sarà oggetto di interferenze arbitrarie nell'ambito della sua vita privata, della famiglia, del domicilio o nella corrispondenza, né a lesione del suo onore o della sua reputazione».

[69] V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 274. Come sottolineano J. VELU–R. ERGEC, *La Convention Européenne des Droits de l'Homme,* Bruylant, 1990, p. 535, «[*A]a n'en pas douter, les concepts utilisès dans cette disposition […] sont extensibles à souhait. Cette flexibilitè, dans le libellè, pour salutaire qu'elle puisse paraitre, n'en suscite pas moins des difficultès d'interprètation. Par ailleurs, à la notion gènèrique de "vie privèe" se succèdent celles de "vie familiale", de "domicile" ed "de Correspondanca". Les trois dernières notions s'analysent, dans une certaine measure, comme des aspects particuliers de la "vie privée" […] Il reste que chacun des droits garantis par l'article 8, § 1er, pose des problèmes suffisamment spècifiques quant à son contenu pour mèriter un examen séparé*».

[70] Si esprime così C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 74.

In passato, alle carenze concettuali e dogmatiche dell'art. 14 Cost., la dottrina suppliva talvolta sovrapponendo la nozione costituzionale con quella fornite dall'art. 43 c.c.[71], talvolta omologandola a quella del diritto penale di cui all'art. 614 c.p.[72].

Per converso, più di recente, gli orientamenti dottrinali sembrano prediligere «un approccio volto ad affermare l'autonomia della nozione costituzionale di domicilio rispetto a quella civile e quella penale»[73], finendo per definirlo come «ogni luogo di cui la persona fisica o giuridica abbia legittimamente la disponibilità per lo svolgimento di attività connesse alla vita privata o di relazione dal quale intenda escludere i terzi»[74].

---

[71] Durante la vigenza dello Statuto albertino, in cui la protezione dell'inviolabilità domiciliare veniva tutelata dall'art. 27, la protezione era accordata «al luogo in cui la persona ha stabilito la sede principale dei propri affari e interessi». In questo senso M. COSTANZA, voce *Domicilio. Il domicilio, residenza e dimora (dir. civ.)*, in *Enc. giur.,* XII, Treccani, 1991, p. 198 ss.

[72] Sulla base di una tradizione consolidatasi durante la vigenza dello Statuto albertino, si riteneva che l'art. 14 Cost. e l'art. 614 c.p. fossero indissolubilmente legati da una comune *ratio* ispiratrice rappresentata dalla libertà individuale. Cfr. P. BARILE, *La libertà nella Costituzione. Lezioni,* Cedam, 1966, p. 149 ss.; P. BARILE–E. CHELI, voce *Domicilio (libertà di*), cit., p. 861 s.; F. CARNELUTTI, *Diritto alla vita privata*, in AA. VV., *Scritti giuridici in onore di P. Calamandrei*, Cedam, 1958, p. 142; V. MANZINI, *Trattato di diritto penale*, Giuffrè, 1964, p. 863 ss.; S. ROMANO, *L'ordinamento giuridico*, Giuffrè, 1962, p. 74, nt. 49; M. SINISCALCO, voce *Domicilio (violazione di),* in *Enc. dir.,* XIII, Giuffrè, 1964, p. 873 ss. Nello stesso senso anche A. SCELLA, *Dubbi sulla legittimità costituzionale e questioni applicative in tema di intercettazioni ambientali in luogo di privata dimora*, in *Cass. pen.,* 1995, f. 3, p. 992 ss.

[73] Così G. AMATO, *Commento all'art. 14 Cost.,* in *Commentario della Costituzione*, cit., p. 61. Allo stesso modo, I. FASO, *La libertà di domicilio*, Giuffrè, 1968, p. 21 s.; E. TRAVERSO, *La libertà di domicilio nella Costituzione italiana,* Giuffrè, 1967, p. 142; M. PISANI, *La tutela penale della "riservatezza": aspetti processuali*, in *Riv. it. dir. proc. pen*., 1967, f. 2, p. 788 ss.

[74] Si esprime così P. CARETTI–U. DE SIERVO, *Istituzioni di diritto pubblico*, p. 602. Anche la giurisprudenza di legittimità tende ad accogliere una nozione ampia di domicilio, sottolineando che «la tutela costituzionale si riferisce non solo alle private dimore e ai luoghi che, pur non costituendo dimora, consentono una temporanea ed esclusiva disponibilità dello spazio ma anche ai luoghi nei quali è temporaneamente garantita un'area di intimità e riservatezza». Così Cass., sez. IV, 16 marzo 2000, n. 7063, in *C.E.D. Cass.,* n. 217689. Nel 2006, in una fondamentale pronuncia relativa all'impiego processuale delle videoriprese di immagini, la Suprema corte amplia la portata del concetto di domicilio, fino a quel momento, per espressa previsione della Consulta, sostanzialmente limitata ad abitazioni private e luoghi analoghi. Cfr. Corte cost., 11 aprile 2002, n. 135, in *Giur. cost.,* 2002, p. 2176 ss. Confermando la distinzione già prospettata tra immagini comunicative e non, la Suprema corte prevede tre differenti discipline a seconda del luogo in cui la captazione è effettuata. Nei luoghi domiciliari le videoriprese di immagini non comunicative sono senz'altro vietate, a pena di inutilizzabilità (a meno che la videoripresa non sia stata effettuata con il consenso della persona offesa. Cfr. Cass., sez. III, 13 giugno 2014, n. 25177, in *www.dirittoegiustizia*, 16 giugno 2014. Ma già sez. III, 7 luglio 2010, n. 37197, in *Guida dir.,* 2010, n. 1, p. 49 ss.; sez. II, 13 dicembre 2007, n. 1127, in *Cass. pen.*, 2009, f. 5, p. 1156 ss.). Nei luoghi riservati, in cui manca la stabilità dello *ius excudendi alios* (esistendo il diritto solo se l soggetto è presente sul luogo) ma sussiste «un'aspettativa di riservatezza maggiore rispetto ai luoghi pubblici», tutelato *ex* art. 2 Cost., sono consentite le videoriprese di immagini non comunicative, purché disposte con provvedimento dell'autorità giudiziaria, fornito di congrua motivazione (sul punto, cfr. sez. I, 10 luglio 2007, n. 31389, in *C.E.D. Cass.,* n. 237502). Così sez. un., 28 luglio 2006, n. 26795, in *Cass. pen.*, 2006, f. 12, p. 4344 ss. In dottrina v. S. BELTRANI, *Le videoriprese? Sono una prova atipica ma le Sezioni unite non sciolgono il nodo*, in *Dir. e giust*., 2006, p. 34 ss.; M.L. DI BITONTO, *Le riprese video domiciliari al vaglio delle Sezioni Unite*, in *Cass. pen.*, 2006, f. 12, p. 3950 ss.; F. RUGGIERI, *Riprese visive e inammissibilità della prova*, *ivi,* 2006, p. 3945. Le videoriprese in luoghi pubblici o aperti o esposti al pubblico, non effettuate nell'ambito del procedimento penale, vanno incluse nella categoria di documenti, *ex* art. 234 c.p.p. Cfr. sez. VI, 17 novembre 2009, n. 36083, in *Guida dir*., 2010, n. 1, p. 90 ss. In base all'evoluzione giurisprudenziale, può dirsi che i luoghi "domiciliari" sono quei luoghi in cui il titolare

Un'ulteriore dilatazione deriva, poi, dall'interpretazione convenzionalmente orientata del concetto: in effetti, la Corte EDU interpreta il diritto all'inviolabilità domiciliare «non solo come diritto all'inviolabilità degli spazi fisici ma anche quale diritto a non subire interferenze nel godimento di quello spazio»[75], ritenendo che la «nozione di domicilio è autonoma e prescinde dalla definizione della legge interna e guarda alla concretezza del rapporto della persona con il luogo»[76].

---

possiede uno *ius excludendi alios* stabile, ovvero azionabile anche quando il soggetto non sia fisicamente presente (il carattere di "stabilità" del diritto risulta, ai fini della determinazione del concetto di domicilio, assolutamente necessario. In proposito la giurisprudenza della Suprema corte ha, ormai, disposto che l'autovettura non può essere considerata un luogo di "privata dimora", in quanto quest'ultima è destinata al trasporto «di persone o al trasferimento di oggetti da un luogo ad un altro ed in quanto sfornito dei confort minimi per potervi risiedere stabilmente per un apprezzabile lasso di tempo […]» Così sez. I, 6 maggio 2008, n. 32851, in *Cass. pen.*, 2009, p. 2533. *Contra* Corte cost., 25 marzo 1987, n. 88, in *Giur. cost.,* 1987, p. 682 s. Tali luoghi rientrano nell'area di tutela dell'art. 14 Cost.: ad ogni modo, affinché scatti la protezione prevista da tale articolo, non basta che un comportamento venga tenuto in un luogo di privata dimora, in quanto occorre che esso sia in concreto riservato, e, cioè non possa in concreto essere liberamente osservato dagli estranei, senza ricorrere a particolari accorgimenti. Cfr. Corte cost., 7 maggio 2008, n. 149, in *Cass. pen.,* 2008, p. 4109. Nello stesso senso anche la giurisprudenza di legittimità, per cui partendo dalla considerazione che il concetto di privata dimora sia *più ampio* di quello di abitazione, vi ricomprende tutti i luoghi al cui interno un soggetto possa vantare un generico *ius excludendi* (vale a dire l'astratta possibilità di inibire l'accesso al pubblico, anche solo in determinati orari) e in cui egli si trattenga per compiere, anche in maniera transitoria e contingente, atti della vita privata, tra i quali pacificamente rientrano anche le attività lavorative di natura professionale, commerciale o imprenditoriale; il delitto di cui all'art. 624 *bis* c.p. è stato così configurato anche in relazione a furti commessi in luoghi quali un ristorante in orario di chiusura, un bar–tabacchi, sempre in orario di chiusura, un cantiere edile allestito all'interno del cortile di un immobile, un'edicola, uno studio odontoiatrico, una farmacia in orario di apertura. Così, rispettivamente, Cass., sez. II, 26 maggio 2015, n. 24763, in *C.E.D. Cass.,* n. 264283; sez. V, 24 novembre 2015, n. 6210, *ivi*, n. 26587; sez. V, 1 ottobre 2014, n. 2768, *ivi*, n. 262677; sez. II, 24 ottobre 2014, n. 46786, *ivi*, n. 261053; sez. V, 17 dicembre 2014, n. 7293, *ivi*, n. 262659; sez. V, 15 febbraio 2011, n. 10187, *ivi*, n. 249850; Cass., sez. IV, 25 giugno 2009, n. 37908, n. 244980. La delicata *quaestio* sembra aver trovato una stabilità ermeneutica grazie al recente apporto delle sezioni unite che accoglie un'interpretazione maggiormente restrittiva alla nozione *de qua*. Cfr. Cass., sez. un., 23 marzo 2017, n. 31345, in *Dir. pen. cont.,* 2017, n. 7–8, con nota di S. BERARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624* bis *c.p.,* secondo cui «rientrano nella nozione di privata dimora di cui all'art. 624 *bis* c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare». Nello stesso senso, sez. IV, 8 agosto 2018, n. 38230, in *www.ilsole24ore.com,* con cui la Suprema Corte eslude dalla nozione di domicilio il pianerottolo di un'abitazione privata. Sul punto, V. BONINI, *Videoriprese investigative e tutela della riservatezza: un binomio che richiede sistemazione legislativa*, in *Proc. pen. giust*., 2019, n. 2, p. 336 ss.

[75] Così M. CARILLO, *El derecho a no ser molestado. Informaciòn y vida privada*, Aranzadi, 2003, p. 44. Nello stesso senso, V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 216. Per questa via si finisce per ricomprendere nella nozione di domicilio anche le sedi sociali, le filiali nonché gli altri locali professionali di pertinenza delle società. Cfr. Corte EDU, sez. II, 15 luglio 2003, *Ernst e altri c. Belgio*, n. 33400/96, §§ 109–117; sez. II, 16 luglio 2002, *Società Colas Est ed altre c. Francia*, n. 37971/97; Grande Camera, 16 dicembre 1992, *Niemietz c. Germania*, n. 13710/88, §§ 27–33. Più in generale, sull'ampiezza della nozione *de qua*, di recente, Corte EDU, sez. IV, 1 marzo 2010, *Demopoulos e altri c. Turchia*, n. 21819/04, § 136; sez. V, 17 ottobre 2013, *Winterstein e altri c. Francia*, n. 27013/07, § 141. Nello stesso senso anche la giurisprudenza della Corte di giustizia dell'Unione europea che estende la tutela dell'art. 7 della Carta Ue anche alle persone giuridiche. Cfr. CGUE, 22 ottobre 2002, *Roquette Frères*, C–94/00.

[76] V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 272.

Pur riconoscendo al precetto *de qua* il valore di diritto "assoluto", sono previste delle deroghe al suo godimento: in particolare, il comma 2 dell'art. 14 Cost., nel trasporre le garanzie contemplate dall'art. 13 Cost. in tema di libertà personale, sembra circoscrivere il novero degli atti restrittivi dell'inviolabilità domiciliare ad un *numerus clausus,* costituito da ispezioni, perquisizioni e sequestri.

Parte della dottrina[77], muovendo dall'omessa indicazione delle intercettazioni tra i mezzi di compressione della libertà domiciliare, sostiene la tesi dell'incompatibilità delle captazioni domiciliari alla Carta fondamentale, ritenendo che debba essere «negata la praticabilità dell'estensione analogica del testo costituzionale, ostandovi il limite logico della eccezionalità della disposizione [...]»[78].

La giurisprudenza, tuttavia, adottando una posizione meno rigorosa, ammette la legittimità costituzionale delle intercettazioni domiciliari sul presupposto di un doveroso bilanciamento tra interessi contrapposti, affermando che «l'inviolabilità del domicilio […] va correlata alla facoltà attribuita alla legge ordinaria di prevedere e regolare intromissioni nel privato anche con la limitazione di ogni forma di comunicazione per atto motivato dell'autorità giudiziaria, limitazione conseguente al privilegio che compete all'interesse pubblico la cui attuazione è demandata al p.m. dalla Costituzione (art. 112 Cost.)»[79].

Allo stato dell'arte, dunque, sono ammesse intercettazioni ambientali domiciliari purché il decreto autorizzativo indichi "specificamente" le situazioni ambientali – ma non, invece, il

---

[77] Cfr. G. TARELLO, *L'interpretazione della legge*, Giuffrè, 1980, p. 134 ss.; ID., *Tecniche interpretative e referendum popolare*, in *Giur. it*., 1978, p. 920. Nello stesso senso, A. SCELLA, *Dubbi di legittimità costituzionale e questioni applicative in tema di intercettazioni ambientali compiute in privata dimora,* cit., p. 997. Più di recente, C. BERTOSSI, *Intercettazioni ambientali e tutela della libertà domiciliare*, in *Dir. pen. proc.,* 2004, f. 3, p. 871 ss.

[78] Si esprime così C. MARINELLI, *Intercettazioni processuali*, cit., p. 76. «Solo una revisione dell'art. 14 Cost. potrebbe consentire captazioni o ingressi clandestini nel domicilio». Così L. FILIPPI, *L'intercettazione di comunicazioni*, cit., p. 59. Va precisato che già oltre quaranta anni fa, alcuni Autori, riferendosi alle interferenze pubbliche non coercitive previste dall'art. 14, comma 3 Cost., accennavano «alla possibilità, tecnologicamente matura, che l'ispezione abbia luogo attraverso l'installazione di (invisibili) apparecchiature, grazie alle quali la si effettui a distanza e senza la consapevolezza del domiciliato», per dire che «un'ispezione come quella ipotizzata non possa mai ricadere sotto la disciplina del comma 3 dell'art. in oggetto e che, quanto
meno, sia sempre coperta da riserva di giurisdizione. Essa infatti, in quanto intrinsecamente idonea a interferire con la segretezza delle comunicazioni, ricadrebbe in ogni caso sotto la rigida disciplina dell'art. 15 Cost.». Così G. AMATO, *Commento all'art. 14 Cost.,* cit., p. 79.

[79] Cass., sez. I, 19 ottobre 1992, n. 4141, in *Cass. pen*., 1995, f. 4, p. 990 ss. Nello stesso senso anche la Consulta. Cfr. Corte cost., 11 aprile 2002, n. 135, cit., per cui il riferimento nell'art. 14, comma 3 Cost. alle ispezioni, perquisizioni e sequestri, anziché esprimere l'intento di tipizzare le limitazioni permesse, troverebbe «spiegazione nella circostanza che gli atti elencati esaurivano le forme di limitazione dell'inviolabilità del domicilio storicamente radicate e positivamente disciplinate all'epoca di redazione della Carta, non potendo evidentemente il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnici successivi». Per un'accurata ricostruzione del dibattito, più di recente, C. PINELLI, *Sull'ammissibilità di restrizioni alla libertà di domicilio e alla libertà di comunicazione tramite* "virus *di Stato*", in *Dir. pen. cont*., 2017, f. 4, p. 75 ss.

luogo[80] – oggetto di intercettazione[81] ovvero, in alternativa, le categorie di persone che possono esserne interessate[82].

[80] La necessità di indicare con precisione il luogo in cui si svolge l'intercettazione tra presenti non è richiesta né dalla legge, né dalla giurisprudenza nazionale o sovranazionale, salvo quando esse debbano avvenire in un domicilio privato. Assolutamente esplicita è stata in proposito la Suprema corte in una sentenza del 1999, secondo cui «l'intercettazione di comunicazione tra presenti richiede l'indicazione dell'ambiente nel quale l'operazione deve avvenire solo quando si tratta di abitazioni o luoghi di privata dimora, secondo l'indicazione di cui all'art. 614 c.p. In tal senso, i locali di uno stabilimento carcerario […] non sono luoghi di privata dimora». Così Cass., sez. VI, 5 novembre 1999, n. 3541, in *C.E.D. Cass.,* n. 214972. Laddove, invece, non si tratti di luoghi di privata dimora, la giurisprudenza ha ritenuto sufficiente l'indicazione della tipologia di ambienti in cui deve essere eseguita l'intercettazione. In questo senso sez. I, 25 febbraio 2009, n. 11506, in *C.E.D. Cass.,* 243044; sez. II, 8 aprile 2014, n. 17894, in *Cass. pen*., 2015, f. 8, 1397. Da ultimo, il principio secondo cui il decreto autorizzativo deve individuare con precisione i luoghi in cui dovrà essere eseguita l'intercettazione delle comunicazioni tra presenti «non solo non è desumibile dalla legge, ma non risulta essere stato mai affermato dalla giurisprudenza e, inoltre, non sembra costituire un requisito significativo funzionale alla tutela dei diritti in gioco, dal momento che la Corte europea dei diritti dell'uomo non ne fa menzione. Nessun riferimento alla indicazione del luogo della captazione». Così sez. VI, 10 marzo 2016, n. 9954, in *www.neldiritto.it.* In questo senso G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti",* in *Dir. pen. cont.,* 7 ottobre 2016, p. 9. In sostanza, la Corte mostra un'apertura al "carattere dinamico" dell'attività di controllo, in riferimento ai diversi ambienti potenzialmente frequentabili dal soggetto ad esso sottoposto. Cfr. sez. VI, 11 dicembre 2007, n. 15396, in *C.E.D. Cass.,* n. 239634 (nel caso di specie l'intercettazione di comunicazioni tra presenti aveva ad oggetto la sala colloqui della casa circondariale in cui si trovava l'imputato e le operazioni di captazione erano proseguite presso la sala colloqui della casa circondariale in cui lo stesso era stato successivamente trasferito); sez. V, 6 dicembre 2011, n. 5956, *ivi*, n. 252137 (la captazione ambientale era stata trasferita dalla vettura oggetto di autorizzazione ad altra vettura successivamente acquistata dall'indagato sottoposto ad intercettazione); sez. IV, 3 maggio 2001, n. 17823, in *Dir. pen. proc.,* 2001, f. 3, p. 876 ss.; sez. VI, 4 settembre 2001, n. 33201, in *Dir. pen. proc*., 2001, f. 5, p. 1380 (nel caso di specie «[...] l'autorizzazione ad intercettare comunicazioni effettuate da un'utenza telefonica mobile in uso all'indagato si estende implicitamente a tutte le utenze che dal medesimo indagato risultino via via attivate mediante la prassi del cambio di scheda»); sez. IV, 11 luglio 2000, n. 4046, in *Giust. pen*., 2001, f. 2, c. 517. Inoltre la Suprema Corte ha anche chiarito che «[...] l'intercettazione ambientale autorizzata in un determinato luogo è stata ritenuta legittimamente disposta anche nelle relative pertinenze». Cfr. Sez. III, 15 dicembre 2010, n. 4178, in *C.E.D. Cass.,* n. 249207. Da ultimo, sez. II, 20 febbraio 2019, n. 19146, in *C.E.D. Cass.,* n. 275583, per cui «[S]sono utilizzabili i risultati delle intercettazioni di comunicazioni tra presenti anche quando nel corso dell'esecuzione intervenga una variazione dei luoghi in cui deve svolgersi la captazione, purché tale variazione rientri nella specificità dell'ambiente oggetto dell'intercettazione autorizzata».

[81] Come rilevato dalla giurisprudenza europea, «[...] il contenuto dell'autorizzazione deve identificare chiaramente la specifica persona da sottoporre a sorveglianza oppure l'unico insieme dei luoghi rispetto ai quali viene ordinata l'intercettazione». Così Corte EDU, sez. IV, 18 maggio 2010, *Kennedy c. Regno Unito*, cit. § 55. Si possono, a questo punto, indicare due punti fermi: da una parte, il decreto autorizzativo delle intercettazioni di comunicazioni tra presenti deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire solo quando si tratta di luoghi di privata dimora, con la limitazione che, in detti luoghi, tale intercettazioni possono essere effettuate «soltanto se vi è fondato motivo di ritenere che in essi si stia svolgendo l'attività criminosa»; dall'altra, per le intercettazioni di comunicazioni tra presenti da espletare in luoghi diversi da quelli indicati dall'art. 614 c.p. deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta. Così Corte EDU, Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, n. 66610/10,§ 27; sez. I, 23 febbraio 2016, *Capriotti c. Italia,* 28819/12, § 44.

[82] Cfr. Corte EDU, Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, cit.

Di qui, la *quaestio* relativa al *quantum* motivazionale del decreto autorizzativo sembra assolutamente centrale, soprattutto in tema di intercettazioni mediante captatore informatico: la «virtuale ubiquità della cimice»[83] mal si concilia con la protezione della sfera domiciliare così come intesa dalla giurisprudenza nazionale ed europea[84]; incompatibilità difficilmente superabile, in quanto strettamente connessa alla natura itinerante del *virus*. Non può essere, infatti, sottaciuto che le intercettazioni tramite *Trojan* non consentono di individuare *ab origine* né i luoghi oggetto della captazione, né tantomeno le categorie di soggetti che potrebbero essere coinvolti[85].

Proprio la Suprema Corte precisa che tali dispositivi «sono divenuti oggetti che accompagnano ogni nostro movimento e ci seguono in ogni luogo» e che perciò «il loro uso come mezzi di intercettazione permette di sottoporre l'individuo ad un penetrante controllo della sua vita: questa sorveglianza si estende, necessariamente, ai soggetti che stanno vicino alla persona interessata», per cui «si impone un difficile bilanciamento delle esigenze investigative, che suggeriscono di fare ricorso a questo strumento dalle potenzialità forse ancora non pienamente esplorate, con la garanzia dei diritti individuali, che possono subire gravi lesioni»[86]. Così, «[I]il carattere itinerante delle nuove spie elettroniche, combinato alla loro potenza d'azione, comporta il rischio di introdursi nella sfera personale di chiunque si trovi ad una certa distanza dal *target*, di captare fortuitamente conversazioni intercorrenti tra terzi, di penetrare in imprevedibili spazi domiciliari di chiunque (non soltanto del soggetto controllato), finanche di intercettare inopitamente su territorio estero»[87].

Non a caso, la giurisprudenza di legittimità, percependo il potenziale *vulnus* al precetto costituzionale della libertà domiciliare delle intercettazioni condotte tramite agente intrusore, ne aveva circosritto la portata, ritenendole ammissibili solo per la prevenzione dei delitti di criminalità organizzata e terrorismo (*ex* artt. 51, commi 3 *bis* e 3 *quater* e 407, comma 2, lett. *a*, n. 4 c.p.p.), in ragione della speciale norma derogatrice di cui all'art. 13 d.l. n. 152 del 1991[88], per cui è legittima la captazione di conversazioni e comunicazioni anche nei luoghi di privata dimora senza necessità di indicare nel provvedimento gli ambienti di esecuzione[89].

---

[83] Così la definisce P. BRONZO, *Intercettazione ambientale,* cit., p. 250.

[84] Sul punto, si consenta un rinvio a Cap. III, § 4.1.

[85] Come precisato, «[…] nelle intercettazioni tradizionali non è mai possibile prevedere chi saranno gli interlocutori; ma in quelle tradizionali, almeno, tali interlocutori sono circoscritti a coloro che conversano su una certa utenza telefonica o, se sono ambientali, a coloro che conversano in deteminati luoghi. Con la captazione informatica si estendono alla folla indeterminata e indeterminabile delle persone, la grande maggioranza delle quali completamente estranee all'indagine, che in qualunque luogo conversano, non necessariamente con il possesso del cellulare, a meno di dieci metri di distanza». Così A. CAPONE, *Intercettazioni e costituzione. Problemi vecchi e nuovi*, cit., p. p. 1270. Nello stesso senso L. FILIPPI, L*'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*., 2016, f. 2, p. 349; A. BALSAMO, *Le intercettazioni mediante* virus *informatico tra processo penale italiano e Corte europea*, cit., p. 2278 ss; G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "tra presenti*", in *Dir. pen. cont*., 7 ottobre 2016.

[86] Cass., sez. un., 28 aprile 2016, n. 26889, in *Cass. pen.,* 2016, n. 10, p. 3546 s.

[87] P. BRONZO*, L'impiego del* trojan horse *informatico nelle indagini penali,* cit., p. 339.

[88] D.l. 13 maggio 1991, n. 152, convertito in l. 12 luglio 1991, n. 203, recante "*Provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza e buon andamento dell'attività amministrativa*", in *Gazz. uff*., 13 maggio 1991, n. 110. Il legislatore, con l'introduzione dell'art. 13 d.l. n. 152/1991, ha inteso favorire l'operatività dell'attività intercettiva in relazione a fattispecie criminose per le quali l'attività di indagine risulta assai complessa: ha, in sostanza, preferito limitare il diritti alla segretezza della corrispondenza e di ogni altra forma di comunicazione e l'inviolabilità del domicilio in relazione all'eccezionale gravità e pericolosità sociale di tali delitti, stante anche le oggettive difficoltà di acquisizione delle prove. Sul punto, v. Cap. I, § 2, nt. 67.

[89] Cfr. Cass., sez. un., 28 aprile 2016, n. 26889, cit., per cui «[I]in tema di intercettazioni di conversazioni o comunicazioni tra presenti, eseguite per mezzo dell'installazione di un "captatore

Di qui, il *renvirement* del legislatore contemporaneo di ampliare il novero delle fattispecie di reato intercettabili mediante il *virus* informatico risulta alquanto fuorviante. Probabilmente, l'approdo minimalista raggiunto qualche tempo prima dalla giurisprudenza di legittimità avrebbe dovuto rappresentare un "modello" per la successiva disciplina, in quanto assai più ragionevole e, soprattutto, compatibile con i dettami costituzionali.

4. IL DIRITTO ALLA RISERVATEZZA E ALLA *PRIVACY* NEL QUADRO DEI DIRITTI FONDAMENTALI

informatico" in dispositivi elettronici portatili deve escludersi la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 c.p., con il mezzo indicato in precedenza, al di fuori della disciplina derogatoria per la criminalità organizzata di cui all'art. 13 d.l. n. 152 del 1991, convertito in legge n. 203 del 1991, non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, comma 2, c.p.p., che in detto luogo "si stia svolgendo l'attività criminosa". È consentita la captazione nei luoghi di privata dimora *ex* art. 614 c.p., pure se non singolarmente individuati e se *ivi* non si stia svolgendo l'attività criminosa, per i procedimenti relativi a delitti di criminalità organizzata, anche terroristica, secondo la previsione dell'art. 13 d.l. n. 152 del 1991. Per procedimenti relativi a delitti di criminalità organizzata devono intendersi quelli elencati nell'art. 51, commi 3 *bis* e 3 *quater*, c.p.p. nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato». Sulpunto, T. ALESCI, *L'intercettazione di comunicazioni o di conversazioni tra presenti con il* Trojan horse *è ammissibile anche nei luoghi di privata dimora per i reati di criminalità organizzata*, in *Proc. pen. giust*., 2016, n. 5, p. 28 ss.; G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un "captatore* informatico*",* in *Guida dir.,* 2016, n. 34–35, p. 76 ss.; S. ATERNO, Digital forensics *(investigazioni informatiche),* cit., p. 217 ss.; G. BARROCU, *Il captatore informatico: un* virus *per tutte le stagioni,* in *Dir. pen. proc*., 2017, n. 3, p. 379 ss.; A. CAMON, *Cavalli di Troia in Cassazione*, in *Arch. n. proc. pen*., 2017, f. 1, p. 91; F. CAJANI, *L'odissea del captatore informatico*, in *Cass. pen*., 2016, n. 11, p. 4139 ss.; S. COLAIOCCO, *Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia*, in *Arch. pen*., 2014, f. 1, p. 1 ss.; P. DI STEFANO*, Grande fratello si, intercettazioni con lo* smartphone *ma solo per la criminalità organizzata*, in *Foro it*., 2016, n. 9, p. 513 ss.; G. LASAGNI, *L'uso di captatori informatici* (trojans) *nelle intercettazioni "fra presenti",* cit.; P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma,* in *Proc. pen. giust*., 2016, n. 5, p. 118 ss.; L. FILIPPI, *L'ispe–perqui–intercettazione "itinerante": le Sezioni Unite azzeccano la diagnosi ma sbagliano la terapia*, cit., p. 348 ss.; S. FURFARO, *Le intercettazioni "ambulanti" nei processi di criminalità organizzata tra garanzie costituzionali ed esigenze di controllo*, in *Arch. pen.,* 2016, n. 2, p. 1 ss.; L. GIORDANO, *Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzioni di garanzia del decreto autorizzativo*, in *Dir. pen. cont.,* 20 marzo 2017; F. GIUNCHEDI, *Captazioni "anomale" di comunicazioni: prova incostituzionale o mera attività di indagine?,* in *Proc. pen. giust*, 2014, n. 1, p. 133 ss.; W. NOCERINO, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale,* in *Cass. pen.,* 2016, n. 10, p. 3549 ss.; M. TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali,* in *Dir. pen. proc*., 2015, f. 9, p. 1163 ss.

Secondo le interpretazioni dottrinali più recenti[90], il diritto alla riservatezza può essere inteso sia come «rispetto all'intimità della vita privata»[91], ossia «all'inaccessibilità della sfera intima

[90] In passato, gli studi volti ad affermare l'esistenza del diritto alla riservatezza riprendono le osservazioni svolte da Warren e Braindeis e definiscono l'interesse al riserbo come «diritto a essere lasciati soli». In particolare, «[L]la riservatezza viene quindi individuata come quello interesse che in base ad una certa valutazione legislativa e sociale risulta fondamentale per l'individuo. Questi ha bisogno per poter condurre la propria vita di vedersi riconosciuto un certo ambito privato dal quale poter escludere l'altrui ingerenza; è la stessa natura umana che rifiuta l'indiscriminata pubblicizzazione di ciò che riguarda nell'intimo. Il rifiuto di tale riconoscimento finirebbe col menomare gravemente l'individuo e col pregiudicare lo stesso valore della persona, quindi la sua dignità; di qui la tutela implicita, anche sotto questo aspetto, del diritto alla riservatezza» Così T.A. AULETTA, *Riservatezza e tutela della personalità*, cit., p. 27. In tema M. BONETTI, *Riservatezza, diritti dell'uomo e processo penale: aspetti problematici,* in *Ind. pen.,* 1995, f. 1, p. 87; A. CERRI, voce *Riservatezza (diritto alla) II) Diritto comparato*, in *Enc. giur.,* XXXVII, Treccani, 1991, p. 3. In senso critico sulla nozione di riservatezza allora esistente, N. LUGARESI, *Internet,* privacy *e pubblici poteri negli Stati uniti*, Milano, 2000, p. 51. Ma già, E. J. BLUOSTEIN, *Privacy an as aspect of human dignity: an aswer: to Dean Prosser*, in *New York University Law Review*, 1964, vol. XXXIX, p. 970. Per ricostruire il dibattito sul diritto alla riservatezza nel nostro ordinamento cfr. F. CARNELUTTI, *Il diritto alla vita privata*, in *Riv. trim. dir. pubbl.*, 1955, f. 1, p. 3; G. GIAMPICCOLO, *La tutela giuridica della persona umana e il cd diritto alla riservatezza,* in *Riv. trim. dir. proc. civ.,* 1958, f. 2, p. 461. Solo successivamente, a partire dagli anni settanta, si è assistito ad una svolta nel pensiero dottrinale. Come osserva S. RODOTÀ, *La* privacy *tra individuo e collettività,* in *Pol. dir.,* 1974, f. 2, p. 551, «esiste una costante relazione tra mutamenti delle tecnologie delle informazioni e mutamenti del concetto di *privacy* che è, infatti, un concetto soggettivo e variabile in funzione dei soggetti, dei momenti storici, dei luoghi». D'altra parte, il contesto di riferimento in cui emerge la nozione di riservatezza è quello ottocentesco, caratterizzato, sul piano sociale, da un forte desiderio di intimità familiare, coniugale e personale. Aspirazione di cui è espressione «la maggiore insofferenza per le costrizioni imposte dalla promiscuità o dal vicinato e il crescente rifiuto della struttura panottica negli edifici di tipo collettivo – prigioni, ospedali, caserme, interrati –, o per dei controlli effettuati sulle persone fisiche». Così M. PERROT, *Modi di abitare*, in AA. VV., *La vita privata*, a cura di P. Ariés–G. Duby, C.D.E. editore, 2001, p. 245. V., altresì, G.B. FERRI, Privacy *e libertà informatica*, in AA. VV., *Banche dati telematiche e diritti della persona,* a cura di G. Alpa–M. Bessone, Cedam, 1984, p. 47; S. RODOTÀ, *La* privacy *tra individuo e collettività,* cit., p. 545. È interessante notare che il percorso seguito in dottrina per giustificare la tutela alla riservatezza ha trovato eco nelle sentenze dei giudici di merito, che già intorno alla metà degli anni cinquanta affermavano l'esistenza nel nostro ordinamento del diritto alla riservatezza, mentre la giurisprudenza di legittimità inizia a parlare espressamente di interesse al riserbo solo dieci anni più tardi. In particolare si ricordano: Trib. Roma, 23 febbraio 1955, in *Foro it*, 1955, f. 1, p. 918 ss.; Trib. Roma, 14 ottobre 1953*, ivi,* 1954, f. 1, p. 115. Le prime decisioni della Corte di Cassazione (Cass., sez. I, 27 maggio 1975, n. 2129, in *Foro it*., 1975, p. 2895 ss.) e della Corte costituzionale (Corte cost., 9 luglio 1970, n. 122, in *Giur. cost*., 1970, p. 1529) adoperano la nozione di "riservatezza". Il termine "*privacy*" compare solo con 1990. Cfr. Corte cost., 26 marzo 1990, n. 139, in *Giur. cost*., 1990, p. 787 ss. Per una ricostruzione dell'evoluzione giurisprudenziale, G. GIACOBBE, voce *Riservatezza (diritto alla),* in *Enc. dir*., XL, Giuffrè, 1989, p. 1243. Nel diritto civile il riconoscimento di un generale diritto alla riservatezza suscettibile di tutela aquiliana, si è imposto – superando la precedente tesi contraria (Cass., sez. I, 22 dicembre 1956, n. 4487, in *Giur. it*., 1957, p. 366) – a seguito della sentenza Cass., sez. III, 27 maggio 1975, n. 2129, in *Foro it.,* 1976, p. 2895. In dottrina, sul riconoscimento del diritto alla riservatezza, *ex plurimis*, T.A. AULETTA, *Riservatezza e tutela della personalità,* cit., p. 42 ss.; M. BONETTI, *Riservatezza e processo penale*, cit., p. 103 ss.; F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza,* in *Riv. it. dir. proc. pen.,* 1967, f. ?, p. 1094 s.; F. CARNELUTTI, *Il diritto alla vita privata*, cit., p. 5 ss.; A. DE CUPIS, *I diritti della personalità*, cit., p. 326; ID., voce Riservatezza e segreto (*diritto a),* in *Noviss. dig. it.,* Utet, 1969, p. 115 ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 78 s.; G. MOROSILLO, *La tutela penale del diritto alla riservatezza*, Giuffrè, 1966, p. 74 ss.; G. GIACOBBE, voce *Riservatezza (diritto alla),* cit., 1243 ss. Per una disamina dei differenti orientamenti, da ultimo, G.

dell'individuo comprensiva delle sue proiezioni spaziali e comunicative»[92] (c.d. riservatezza in senso stretto), sia quale «potere di controllare e gestire ogni informazione personale»[93] (c.d. *privacy*). Da ciò si desume che, se da un lato il termine "riservatezza in senso stretto" contempla tutte le situazioni che prospettano un'esigenza di tutela dell'intimità personale, dall'altro, il termine "*privacy*" individua circostanze più complesse «che finiscono per simboleggiare l'insieme delle libertà che sono implicate nel trattamento dei dati personali»[94] (c.d. *habeas data*)[95].

Pur se legate da un rapporto di genere a specie, può dirsi che tanto la riservatezza quanto la *privacy*, si stagliano quali «diritti dell'uomo a sé stanti»[96], tutelati in quanto tali dal sistema giuridico «che li presuppone a se stesso»[97] e che «entrambe le prerogative si ergono a paradigma della categoria dei c.d. diritti "liquidi", ossia anamorfici o metamorfici in quanto privi di connotati durevoli e stabili […]»[98].

Una volta delineato il contenuto dei precetti in esame, sembra doveroso esaminare la peculiare natura giuridica dei «nuovi diritti»[99] al fine di poterli annoverare, senza alcuna riserva, nel *genus* delle prerogative fondamentali di ogni individuo[100].

VISINTINI, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Dir. inf. e inf*., 2019, f. 1, p. 1 ss.

[91] In questo senso F. RESCIGNO, *Il diritto all'intimità della vita privata*, in *Studi in onore di F. Santoro Passarelli,* Jovene, 1993, p. 119.

[92] F. CAPRIOLI, *Colloqui riservati e prova penale*, cit., p. 16.

[93] Cfr. S. RODOTÀ, *La* privacy *tra individuo e collettività,* cit., p. 547. Nello stesso senso, L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislative e beni giuridici tutelati*, in AA. VV., *Il diritto penale dell'informatica nell'epoca di internet*, a cura di L. Picotti, Cedam, 2005, p. 77. Più di recente M. TORRE, Privacy *e indagini penali,* Giuffrè, 2020, p. 7 ss. Più di recente, L. LUPARIA, *Diritto alla* privacy, in AA. VV., *Diritti della persona e nuove sfide del processo penale,* cit., p. 98 ss. In giurisprudenza, solo a titolo esemplificativo, Corte EDU, Grande Camera, 4 maggio 2000, *Rotaru c. Romania*, n. 28341/95; Grande Camera, 4 dicembre 2008, *Marper c. Regno Unito,* n. 30562/04 e 30566/04; sez. III, 25 febbraio 1997, *Z. c. Finlandia,* n. 22009/93, §§ 95–96. Ma già, Grande Camera, 26 marzo 1987, *Leander c. Svezia,* cit.

[94] Si esprime così S. RODOTÀ, voce *Riservatezza,* cit. Nello stesso senso, S. NIGER*, Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, cit., p. 43.

[95] L'*habeas data* è definibile come corollario dell'*habeas corpus*: esso impone che la raccolta e l'analisi organizzata dei dati debba avvenire secondo precise regole, sul presupposto che «noi siamo i nostri dati […], le persone hanno sempre più bisogno di una tutela del loro "corpo elettronico"». Così S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2014, p. 44. V., altresì, ID, *Libert*à *personale. Vecchi e nuovi nemici*, in AA. VV., *Quale libertà. Dizionario minimo contro i falsi liberali*, a cura di M. Bovero, Laterza, 2004, p. 52 s. Nello stesso senso, V. FROSINI, *Il giurista e le tecnologie dell'informazione*, Bulzoni, 2000, *passim*; G. PINO, *Il diritto all'identità personale ieri e oggi*. *Informazione, mercato, dati personali*, in AA. VV., *Libera circolazione e protezione dei dati personali,* a cura di R. Panetta, Giuffrè, 2006, p. 257 ss.

[96] Così C. MORTATI, *Istituzioni di diritto pubblico*, Cedam, 1976, p. 1067.

[97] M. BONETTI, *Riservatezza e processo penale*, cit., p. 59.

[98] L'espressione appartiene a A. CISTERNA, *Cedu e diritto alla* privacy, in AA. VV., *I principi europei del processo penale*, cit., p. 194. Ma già S. RODOTÀ, *La* privacy *tra individuo e collettività*, cit., p. 551.

[99] F. MODUGNO, *I "nuovi diritti" nella giurisprudenza costituzionale*, Giappichelli, 1995, p. 21.

[100] Quello dell'inclusione del diritto alla riservatezza nell'ambito dei diritti dell'uomo è un argomento assai dibattuto in dottrina. In chiave comparatistica, *ex multis*, AA. VV., *Encyclopedia of human rights*, Editor in Chief, 1995; AA. VV., *Human rights: concept and standards*, a cura di J. Symonides, Routledge, 2000; AA. VV., *Promoting human rights through bills of rights: comparative prospectives*, P. Alston, 1999; M. PATRONO, *I diritti dell'uomo nel paese d'Europa,* Cedam, 2000, p. 23 ss.; D. ROBERTSON, *A dictionary of Human Rights*, Routledge, 2004; L. SHELTON, *Remedies in International human rights law*, OUP Oxford, III ed., 2015. In ambito nazionale, tra i contributi più significativi, A. BALDASSARRE, voce *Diritti inviolabili*, cit., p. 17 ss.; G. BOGNETTI, voce *Diritti dell'uomo*, in *Dig. disc. priv*., V, Utet, 1989, p. 383 ss.; S. CASSESE, *I diritti umani nel mondo contemporaneo*, Laterza, 1988;

Il punto di partenza dell'analisi del diritto alla riservatezza non può non essere «l'ingenua costatazione»[101] della mancata previsione, nell'assetto costituzionale nazionale, della protezione della vita privata.

All'assenza di qualsivoglia tutela costituzionale, la dottrina risponde attribuendogli una protezione "indiretta"[102]: a chi[103] ritiene che il suo fondamento sia rappresentato dall'art. 2 Cost., in quanto norma "aperta" in grado di «esprimere la carica espansiva della Carta fondamentale»[104], si contrappone l'orientamento seguito da coloro che lo rintracciano nell'art. 3 Cost., facendo leva sui concetti di «dignità e pieno sviluppo della persona»[105].

Una posizione intermedia è, invece, quella che, pur riconoscendo all'art. 2 Cost. la funzione di assicurare una tutela di carattere generale ai diritti della personalità, anche a prescindere da una previsione espressa, delinea margini di protezione specifica della riservatezza attraverso un «procedimento di derivazione da quelle disposizioni che hanno ad oggetto valori ad essa direttamente riferibili, poiché ne rappresentano aspetti particolari»[106].

Secondo tale prospettiva, il diritto al rispetto della vita privata troverebbe tutela implicita dagli artt. 13, 14 e 15 Cost., posti a presidio del complesso dei diritti della personalità[107];

G.M. FLIK, *Globalizzazione e diritti umani*, in *Jus*, 2000, p. 172 ss.; D. MESSINETTI, voce *Personalità (diritti della),* in *Enc. dir*., XXXIII, Giuffrè, 1983, p. 355 ss.

[101] Si esprime così G.M. SALERNO, *La protezione della riservatezza e l'inviolabilità della corrispondenza*, cit., p. 429.

[102] Una parte minoritaria di dottrina dubita del rango costituzionale del diritto. In questo senso E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche e ambientali*, *Innovazioni tecnologiche e nuovi questioni giuridiche*, cit., p. 160; M. PISANI, *La tutela penale della "riservatezza": aspetti processuali*, cit., p. 784 s.

[103] Cfr. M. BONETTI, *Riservatezza e processo penale*, cit., p. 103; A. CAUTADELLA, voce *Riservatezza*, in *Enc. giur.*, XXVI, Treccani, 1965, p. 2. V., altresì, F. BRICOLA, *Prospettive e limiti della tutela penale della riservatezza*, cit., p. 1067.

[104] Così A. BALDASSARRE, voce *Diritti inviolabili*, cit., p. 18. Nello stesso senso, A. BARBERA, *Commento all'art. 2 Cost.,* in *Commentario alla Costituzione*, cit., p. 102. Propendono per l'ampiezza della sfera di operatività dell'art. 2 Cost., P. BARILE, *Diritti dell'uomo e libertà fondamentali*, cit., p. 52; P. CARETTI–U. DE SIERVO, *Istituzioni di diritto pubblico*, cit., p. 594 s.; C. MORTATI, *Istituzioni di diritto pubblico*, cit., p. 1038; A. PACE, *Problematiche delle libertà costituzionali*, cit., p. 3; G. VASSALLI, *Il diritto alla libertà morale,* in AA. VV., *Studi in memoria di F. Vassalli*, Utet, 1960, p. 1640. Nello stesso senso anche la giurisprudenza costituzionale. Cfr. Corte cost., 27 giugno 1996, n. 223, in *Giur. cost*., 1996, p. 1918; 23 luglio 1996, n. 297, *ivi*, 1996, p. 2475; 24 gennaio 1994, n. 13, *ivi*, 1995, p. 95; 10 febbraio 1988, n. 183, *ivi*, 1988, p. 687; 24 marzo 1986, n. 54, *ivi*, 1987, p. 387. *Contra*, P. GROSSI, *Introduzione a uno studio sui diritti inviolabili nella Costituzione italiana*, Cedam, 1972, p. 172. Più di recente, G. DE VERGOTTINI, *Oltre il dialogo tra le Corti. Giudici, diritto straniero e comparazione*, Il Mulino, 2010, p. 149 s.; S. SCAGLIARINI, *La riservatezza e i suoi limiti. Sul bilanciamento di un diritto preso troppo sul serio*, Aracne, 2013, p. 141 ss.

[105] T.A. AULETTA, *Riservatezza e tutela della personalità*, cit., p. 42 ss.; G. BUSIA, voce *Diritto alla riservatezza*, in *Dig. disc. pubbl.,* IV, Utet, 2000, p. 46 ss.; A. MANNA, *Riservatezza, arte e scienza: quid iuris?,* in *Dir. informazione e informatica*, 1986, p. 513; F. MANTOVANI, *Diritto alla riservatezza e libertà di manifestazione del pensiero con riguardo alla pubblicità dei fatti criminosi*, in *Arch. giur.,* 1968, p. 57; M. MAZZIOTTI, *Diritto all'immagine e Costituzione*, in *Giur. cost*., 1970, p. 1534; G. MORSILLO, *La tutela penale del diritto alla riservatezza,* Giuffrè, 1966, p. 74.

[106] C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 83.

[107] In questo senso A. BALDASSARRE, voce *Diritti inviolabili*, cit., p. 20; A. BARBERA, *I principi costituzionali e libertà personale*, Giuffrè, 1971, p. 119; ID., *La libertà tra "diritti" e "istituzioni*", in AA. VV., *Aspetti e tendenze del diritto costituzionale. Studi in onore di Costantino Mortati*, Giuffrè, 1977, p. 12 ss.; P. BARILE, *Diritti dell'uomo e libertà fondamentali,* cit., p. 61; M. BONETTI, *Riservatezza, diritti dell'uomo e processo penale: aspetti problematici*, in *Ind. pen.,* 1995, p. 594; F. CARDACI–S. OLIVETTI, *Il diritto alla riservatezza in Italia*, in *www.jus.unitn.it;* P. CARETTI, voce *Libertà personale*, in *Dig. disc. pubb*., IX, Utet, 1994, p. 231 ss.; A. CISTERNA, *Cedu e diritto alla* privacy, cit.,

impostazione, questa, «meritevole di adesione perché, nel commensurare il *quantum* di tutela all'eterogeneità dei profili di volta in volta in considerazione, coglie la precisa opzione normativa sottesa alla tecnica redazionale dei costituenti, scongiurando i rischi contrapposti legati, da un lato, ad un'eccessiva cristallizzazione dei valori tutelati e dall'altro ad una ricostruzione riduttiva del concetto di riservatezza»[108].

A questo punto, di fronte alla dinamica evolutiva di tale nozione, non pare superfluo vagliare se la protezione dei dati personali, anch'essa del tutto assente nella Carta fondamentale, si attagli quale nuovo diritto di rango e valore costituzionale.

In senso negativo, potrebbe argomentarsi che l'inclusione tra i diritti inviolabili dell'uomo proclamata dalla Corte Costituzionale sia riferita esclusivamente alla riservatezza concepita come «tutela del riserbo sulle vicende personali prive di rilevanza sociale»[109], mentre analoghe conferme non si hanno per il diritto alla protezione dei dati di carattere personale.

Nella direzione opposta, interpretando in senso evolutivo le norme costituzionali, si potrebbe ritenere che il diritto alla *privacy* sia ricompreso tra i diritti inviolabili della persona e, quindi, tutelato dall'art. 2 della Costituzione[110]: «[I]in questa prospettiva l'art. 2 Cost. non è più una formula riassuntiva dei diversi diritti della persona costituzionalmente riconosciuti, ma una clausola generale attraverso la quale operare il continuo adeguamento delle garanzie giuridiche alle sempre nuove esigenze di tutela della persona»[111].

L'ipotesi or ora richiamata sembra maggiormente coerente agli orientamenti sistematici moderni che interpretano il diritto alla riservatezza come comprensivo del diritto alla *privacy*:

---

p. 146 ss.; G. MORSILLO, *La tutela penale del diritto alla riservatezza,* cit., p. 67 ss. In giurisprudenza, Corte cost. sent. 6 aprile 1973, n. 34, in *Giur. cost.,* 1973, p. 316, e 24 aprile 2002, n. 135, cit. Nello stesso senso anche i giudici di legittimità. Cfr. Cass, sez. un., 28 marzo 2006, n. 26759, in *Cass. pen.,* p. 3937 ss.

[108] Si esprime così C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, cit., p. 84. La tutela del diritto al rispetto della vita privata si propone come momento di tutela generale della persona e ciò assume particolare rilievo laddove si consideri che le situazioni e le relazioni poste in essere dall'individuo sono, per un verso, espressione del diritto del singolo ad intrattenere rapporti e, per un altro, esse stesse oggetto di tutela laddove autonomamente considerate. In forza di una impostazione che estende, senza sovrapporre, la tutela del singolo a quella dei rapporti che egli intrattiene, nel caso in cui determinate relazioni non siano considerate come autonomo oggetto di tutela, esse vengono comunque ricomprese nel generale portato della tutela individuale. Per l'effetto, tutte le situazioni individuali, diverse da quelle considerate dalla norma alla stregua di specifico oggetto di tutela, sono ricomprese nella più generale tutela della "vita privata" che costituisce l'oggetto di un fondamentale diritto, distinto e diverso dagli altri. Cfr. A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, cit., p. 371.

[109] Sul punto, Corte cost., 10 febbraio 1994, n. 63, in *www.giurcost.org*; 26 febbraio 1993, n. 81, *ivi*; 11 luglio 1991, n. 366, in *www.cortecostituzionale.it*; 7 maggio 1975, n. 120, in *www.giurcost.org*; 5 aprile 1973, n. 38, *ivi*; Corte cost., 19 aprile 1972, n. 63, in *Giur. cost*., 1972.

[110] In questo senso T.A. AULETTA, *Riservatezza e tutela della personalità*, cit., p. 42 ss.; P. BARILE, *Diritti dell'uomo e libertà fondamentali,* cit., p. 112 ss.; A. BALDASSARRE, voce *Diritti inviolabili*, cit., p. 19 s.; A. BARBERA, *I principi costituzionali e libertà personale*, cit., p. 190 ss.; A. PACE, voce *Libertà personale (dir. cost.)*, cit., p. Più di recente, S. RODOTÀ, *La rivoluzione della dignità*, La scuola di Pitagora, 2013, p. 37 ss.

[111] S. NIGER, *Le nuove dimensioni della* privacy: *dal diritto alla riservatezza alla protezione dei dati personali,* cit., p. 43. Come sostenuto, «tale disposizione consente per struttura e ratio, l'individuazione delle situazioni di vantaggio che, a prescindere da qualsivoglia indicazione esplicita, risultano essere congeniali al libero sviluppo della persona umana». Così A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, cit., p. 369.

attribuendo al primo valore costituzionale, automaticamente non può ritenersi escluso dal *genus* dei principi inviolabili anche il novello diritto alla privatezza[112].

Se il riconoscimento del diritto alla riservatezza e alla *privacy* nel quadro delle garanzie costituzionali nazionali rappresenta il fulcro del dibattito giurisprudenziale e dottrinale nazionale, la *quaestio* non pare interessare il diritto internazionale pattizio, dal momento che la tutela della vita privata e dei dati personali viene espressamente riconosciuta nelle Carte fondamentali[113].

In particolare, la tutela della riservatezza trova protezione nell'art. 8 CEDU che, al primo paragrafo, accanto ai più specifici diritti di libertà delle comunicazioni e domiciliare, garantisce «il rispetto della vita privata e familiare»[114], nonché nell'art. 16, paragrafo 1 del TFUE[115] che consacra il diritto individuale alla protezione dei dati personali.

Nonostante la previsione esplicita della tutela, la portata e il contenuto del precetto sono stati progressivamente definiti dalla giurisprudenza della Corte europea che ha esteso notevolmente il suo ambito applicativo[116], finendo per affermare che rientri nella previsione della norma *de qua*

---

[112] R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in AA. VV., *Diritto alla riservatezza e circolazione dei dati personali,* a cura di R. PARDOLESI, Giuffrè, 2003, p. 44; E. VARANI, *Il "nuovo" diritto alla* privacy. *Dalla Carta di Nizza al Codice in materia di protezione dei dati personali,* in *Dir. cost.,* 7 aprile 2012.

[113] In questo senso M. NINO, *Terrorismo internazionale*, privacy *e protezione dei dati personali,* ESI, 2012, p. 34 s. Per una panoramica sul diritto alla privacy in ambito europeo e sulle origini del diritto *de qua*, AA. VV., *La nuova disciplina europea della* privacy, a cura di S. Sica-V. D'Antonio-G.M. Riccio, Wolters Kluwer-Cedam, 2016.

[114] Il diritto contemplato dall'art. 8 CEDU può essere definibile come "riservatezza" in senso lato, ovvero come "privatezza", concernendo sia le notizie personali non conoscibili da terzi, sia le notizie non divulgabili da chi le abbia conosciute lecitamente ma senza il consenso dell'interessato (riservatezza in senso specifico). In questo senso M. BONETTI, *Riservatezza e processo penale*, cit., p. 112 ss.; G. UBERTIS, *Sistema di procedura penale. Principi generali*, Giuffrè, 2013, p. 202 ss. Così anche S. LORUSSO, *L'arte di ascoltare e l'investigazione penale tra esigenze di giustizia e tutela della* privacy, in *Dir. pen. proc*., 2011, f. 11, p. 1399 ss. Assai interessanti appaiono anche le ricostruzioni della dottrina internazionalistica. Cfr. A. TERRASI, *Information Exchange and Data Protection in Security Matters. The Legal Framework in the Eu–ropean Union and in the Relationship Between the EU and the US*, in AA. VV*., La gouvernance globale face aux défis de la sécurité collective/Global Governance and the Challenges of Collective Security*, a cura di M. Arcari–L. Balmond, Editoriale Scientifica, 2012, p. 213 ss.

[115] Il Trattato sul Funzionamento dell'UE è considerato, insieme al Trattato sull'Unione Europea (TUE), la base fondamentale del diritto primario nel sistema politico dell'UE. l TFUE risale al trattato sulla fondazione della Comunità economica europea, stipulato a Roma nel 1957, ma da allora, ha subito numerose modifiche, a ultimo, per opera dall'articolo 2 del trattato di Lisbona del 13 dicembre 2007 e ratificato dall'Italia con legge 2 agosto 2008, n. 130, recante "*Ratifica ed esecuzione del Trattato di Lisbona che modifica il Trattato sull'Unione europea e il Trattato che istituisce la Comunità europea e alcuni atti connessi, con atto finale, protocolli e dichiarazioni, fatto a Lisbona il 13 dicembre 2007*", in *Gazz. uff*., 8 agosto 2008, n. 185.

[116] Come sostenuto dalla dottrina dominante, «non è possibile [fornire] una definizione esaustiva e definitiva della vita privata individuale e sociale di cui ciascuno deve poter godere», in quanto il diritto al rispetto della vita privata rinvia all'autonomia e alla dignità, all'identità e alla protezione della riservatezza della persona, al diritto all'autodeterminazione individuale. Così V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali in Europa*, cit., p. 249. Nello stesso senso, S. CARNEVALE, *Autodeterminazione informativa e processo penale: le coordinate costituzionali*, in AA. VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?,* a cura di D. Negri, Aracne, 2007, p. 3 ss.; M. LOSANO, *Dei diritti e dei doveri: anche nella tutela della* privacy, in AA. VV., *La legge italiana sulla* privacy. *Un bilancio dei primi cinque anni,* a cura di M. Losano, Laterza, 2001, p. VIII; B. MARKESINIS–G. ALPA, *Il diritto alla* privacy *nell'esperienza di* common law *e nell'esperienza italiana*, in *Riv. trim. dir. proc. civ.,* 1997, p. 417 ss.; R. PAGANO, *Tutela dei dati personali: evoluzione della legislazione europea e stato del dibattito*, in *Inf. e dir.,* 1986, p. 67 ss.; R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una*

«qualsiasi limitazione al rispetto della vita privata»[117], specificando che ogni intromissione riveste di per sé la caratteristica di «ingerenza della pubblica autorità nella sfera privata e ciò anche quando di essa non si sia fatto un uso processualmente rilevante»[118].

Tuttavia, il diritto alla riservatezza e alla *privacy*, così come delineato dalla giurisprudenza della Corte EDU, non è tutelato in modo assoluto: come noto, il paragrafo 2 dell'art. 8 CEDU ne ammette la possibile restrizione da parte della pubblica autorità, purché l'intervento si sostanzia in misure necessarie in una società democratica a perseguire interessi collettivi (quali la sicurezza nazionale, l'ordine pubblico, il benessere economico, la prevenzione dei reati) o individuali (la protezione di diritti e libertà altrui).

---

storia di evoluzione e discontinuità, cit., p. 3 ss.; E. ROPPO, *I diritti della personalità,* in AA. VV., *Banche dati, telematica e diritti della persona*, Cedam, 1984, p. 60 ss.; A. SENESE, *Il diritto alla riservatezza nella prospettiva del diritto costituzionale europeo*, in AA. VV., *Il diritto costituzionale comune europeo,* a cura di M. Scudiero, Jovene, 2002, p. 1343 ss. Più di recente, D. CALDIROLA, *Il diritto alla riservatezza,* cit., p. 59 ss.; S. NIGER*, Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, cit., p. 62. Da ultimo, M. BONETTI–A. GALLUCCIO, sub *art. 8 CEDU. Profili specifici*, cit., p. 262, Tra le pronunce che hanno contribuito a fornire una definizione di vita privata e familiare, Corte EDU, sez. IV, 20 maggio 2014, *McDonald c. Regno Unito*, n. 4241/12, §§ 46–47; Grande Camera, 12 giugno 2014, *Fernandez Martinez c. Spagna*, n. 56030/07, §§ 109–113; sez. IV, 20 luglio 2010, *Dadouch c. Malta*, n. 38816/07, §§ 47–51; sez. V, 23 settembre 2010, *Schuth c. Germania*, n. 1620/03, § 53. Ma già Grande Camera, 9 ottobre 2003, *Slivenko c. Lettonia*, n. 48321/99, §§ 93–98; Grande Camera, 11 luglio 2002, *Christine Goodwinw c. Regno Unito*, n. 28957/95, § 90.

[117] Corte EDU, sez. III, 12 maggio 2000*, Khan c. Regno Unito*, n. 35394/97. Nello specifico, in tema di intercettazioni telefoniche e ambientali, Grande Camera, 12 maggio 2005*, Ocalan c. Turchia*, n. 46221/99; sez. II, 20 dicembre 2005, *Wisse c. Francia*, n. 71611/01; sez. III, 14 marzo 2002, *Puzinas c. Lituania*, cit.

[118] In questo senso Corte EDU, Grande Camere, 25 marzo 1998, *Kopp c. Svizzera*, cit., § 44; Grande Camera, 15 giugno 1992, *Ludi c. Svizzera*, n. 12433/88, secondo cui «basta constatare che i dati relativi alla vita privata sono stati raccolti da una autorità pubblica» per concludere che la loro sistemazione e la conservazione «costituiscono una ingerenza, ai sensi dell'art. 8». In senso analogo anche Grande Camera, 4 maggio 2000, *Rotaru c. Romania*, cit. Più in generale, può sostenersi che tutte le situazioni individuali, diverse da quelle considerate dalla norma come specifico oggetto di tutela (ossia il "domicilio", la "corrispondenza", la "vita familiare), convergono nella più generale nozione di "vita privata". Sul tema, A. CISTERNA, *Cedu e diritto alla* privacy, cit., p. 218 ss. In giurisprudenza, Corte EDU, sez. II, 20 dicembre 2005, *Wisse c. Francia*, cit., § 34, secondo cui «[…] la vita privata è una nozione ampia che non si presta ad una definizione esaustiva [posto] che esiste una zona di interazione tra l'individuo e gli altri che, nonostante il contesto pubblico nel quale si svolge, può considerarsi come vita privata. […]. Un certo numero di elementi entrano in gioco per determinare se la vita privata di una persona è toccata da misure di sorveglianza e controllo prese al di fuori del suo domicilio. […]. Una persona che cammina sulla strada sarà necessariamente vista da tutte le altre persone che vi si trovano. Il fatto che questa scena sia ripresa con mezzi tecnici riveste identico carattere. Diversamente, però, la creazione di un sistema di registrazione permanente di tali elementi che, pur appartenenti alla vita pubblica, può dar luogo a lesione della vita privata […] quando la sorveglianza dell'agire di un individuo in luogo pubblico sia utilizzata per fini diversi da quelli per i quali è stata disposta in base alla legge». In senso conforme già, sez. IV, 28 gennaio 2003, *Peck c. Regno Unito*, n. 44647/98; sez. III, 17 luglio 2003, *Perry c. Regno Unito*, n. 63737/00. In realtà, la Corte già nel 1978, amplia la sfera di tutela dell'art. 8 CEDU fino a ricomprendere il mero reperimento e catalogazione dei dati inerenti all'individuo, a meno che non siano determinate da ragioni di sicurezza e ordine pubblico. Cfr. Grande Camera, 26 marzo 1987, *Leander c. Svezia* cit., per cui «la memorizzazione da parte di un'autorità pubblica dei dati relativi alla vita privata di un individuo costituisce una ingerenza ai sensi dell'art. 8. L'utilizzazione ulteriore delle informazioni memorizzate *importe peu*». In senso conforme, anche Grande Camere, 25 marzo 1998, *Kopp c. Svizzera.*

In sostanza, nella verifica della compatibilità dell'ingerenza statale al diritto al rispetto della vita privata e familiare, la Corte opera un complesso bilanciamento tra i contrapposti interessi in gioco, valutando se la misura adottata dallo Stato aderente, oltre che provvista di una base legale, sia proporzionata e necessaria per proteggere gli interessi pubblici indicati nella clausola derogatoria[119].

Altrettando ampia e compiuta appare la disciplina del diritto alla riservatezza contenuta nella Carta dei diritti dell'Unione Europea che garantisce una tutela *ad hoc* sia al diritto al rispetto della vita privata (art. 7) che al diritto alla protezione dei dati personali (art. 8)[120]; nonché dagli artt. 12 della Dichiarazione Universale dei diritti umani e 17 del Patto internazionale sui diritti civili e politici[121].

Alla luce delle considerazioni or ora svolte, non v'è dubbio che il complesso di attività investigative (sia intercettive che esplorative) condotte tramite *virus* informatico possano compromettere il precetto *de quo.* Si è detto, infatti, che l'invasività delle intercettazioni è, per

[119] La giurisprudenza europea consacra il principio principio della finalità limitata ed il riconoscimento di situazioni giuridiche attive agli interessati dal trattamento delle informazioni apprese, secondo cui i dati personali devono essere rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Questo principio richiede, in particolare, che il legislatore indichi in maniera chiara e precisa le finalità sottese al trattamento dei dati, per evitare che il trattamento stesso perse gua scopi talmente ampi da giustificare una ingerenza arbitraria e ingiustificata nella *privacy* individuale di chi vi sia sottoposto. Corte EDU, Grande Camera, 26 marzo 1987, *Leander c. Svezia,* cit. Nello stesso senso, sez. III, 17 luglio 2003, *Perry c. Regno Unito*, cit; sez. IV, 18 settembre 2014, *Brunet c. Francia*, n. 21010/10, §§ 31–45. In dottrina, *ex multis*, S. ALLEGREZZA, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione Europa*, in AA. VV., *Protezione dei dati personali e accertamento penale,* cit., p. 65 ss.; A. BALSAMO, *Il contenuto dei diritti fondamentali,* in AA. VV., *Manuale di procedura penale europea*, cit., p. 99 ss.; L. D'ANDRIA, *Ragionevolezza e legittimazione del sistema*, Giuffrè, 2005, p. 55; A. GAITO–S. FURFARO, *Intercettazioni,* cit., p. 377 ss.; M. NINO, *Il caso* Datagate: *i problemi di compatibilità del programma di sorveglianza* PRISM *con la* nrmativa europea sulla protezione dei dati personali e *della* privacy, in *Dir. umani e dir. internaz*., 2013, f. 3, vol. 7, p. 729 ss.; V. ZAGREBELSKY–R. CHENAL–L. TOMASI, *Manuale dei diritti fondamentali*, cit., p. 130 ss.

[120] Rispetto all'art. 8 CEDU, la scelta, fatta nella Carta di Nizza, di approntare una protezione separata a situazioni diverse, in cui il singolo definisce la propria sfera personale, consente di recepire un ricchissimo patrimonio giurisprudenziale elaborato nel corso dei decenni dalla Corte Europea con le proprie decisioni, che hanno fornito una lettura "vivente" del testo elaborato nel 1950 al passo con l'evoluzione sociale, economica e culturale. F. PIZZETTI, *La* privacy *come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in AA. VV., *La nuova Europa dopo il Trattato di Lisbona*, a cura di P. Bilancia–M. D'Amico, Giuffrè, 2011, p. 85. Tuttavia, la distinzione nasce verosimilmente «in conseguenza della traslatizia autonoma regolamentazione» della tutela dei dati personali già contemplata nell'art. 286 TCE e ora negli artt. 39 TUE e 16 TFUE. Così G. UBERTIS, *Sistema di procedura penale*, cit., p. 202. In giurisprudenza, CGUE, 12 novembre 1969, *Erich Stauder c. Città di ULM – Sozialamt,* C–29 /69; 14 maggio 1974, *J. Nold Kohlen–und Baustoffgrobhandlung c. Commissione*, C–4/73; 13 dicembre 1979, *Liselotte Hauer c. Land Rheinland– Pfalz,* C–44/79; 13 luglio 1989, *Haubert Wachauf c. Germania,* C–5/88. La Corte ha comunque chiarito che il diritto alla protezione dei dati personali e il diritto al rispetto della vita privata, sono da considerare due volti della medesima medaglia, in quanto interdipendenti e connessi tra loro. Cfr. CGUE, 9 novembre 2010, *Volker*, C–92/09 e C 93/09, § 47. Nello stesso senso, più di recente, 6 ottobre 2015, *Maximilian Schrems – Data Protection Commissioner*, in *Giur. cost*., 2016, p. 273, con nota di R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europeo della* privacy.

[121] Per dovere di completezza, va detto che l'art. 17 del Patto riprende integralmente l'art. 12 della Dichiarazione e così pure l'art. 8 CEDU, che si caratterizza per proporre indicazioni, anche derogatorie, dirette al legislatore interno al fine della predisposizione di una disciplina interna adeguata rispetto all'ampia portata del diritto.

definizione, il contraltare al diritto alla riservatezza[122] «che in questo settore trova la sua apicale compressione e, nel contempo, la sua significativa regolamentazione»[123].

Certamente, questo mezzo di ricerca della prova può considerarsi fondamentale durante l'esecuzione delle indagini preliminari quale contraltare all' «ingèniosità»[124] del comportamento criminoso ma fuoriesce dai limiti del consentito ogni qual volta non vi sia tutela contro gli eccessi, come avviene nel caso in cui non siano previste garanzie sufficienti in relazione ai soggetti terzi occasionalmente coinvolti, alla "tipologia" di informazioni apprese, ai tempi, ai luoghi oggetto di captazione.

Di qui, se l'intromissione nella sfera di riservatezza può essere "tollerata" nel caso delle intercettazioni "tradizionali", presidiate da specifiche garanzie legislative e giurisdizionali, non altrettanto può farsi in relazione a quelle captazioni più avanguardistiche, per cui i presidi normativi risultano alquanto labili e sfumati.

---

[122] Il diritto alla riservatezza viene considerato come un "diritto di seconda generazione" che si sviluppa in risposta ai nuovi bisogni sociali sorti a seguito del progresso tecnologico e scientifico. Più in particolare, l'esigenza di tutelare la riservatezza individuale inizia a emergere, in dottrina, per la prima volta negli Stati Uniti alla fine del XIX secolo, allorquando il fenomeno dell'industrializzazione favorisce lo sviluppo e la ricerca tecnologica. In questo contesto, la classe borghese, insoddisfatta di vedere tutelato il solo diritto di proprietà, comincia a sentire il bisogno di vedere protetta anche la propria sfera intima. Sull'origine del diritto alla riservatezza*, ex multis,* D. CALDIROLA, *Il diritto alla riservatezza,* Cedam, 2006, p. 5 ss.; S. NIGER*, Le nuove dimensioni della* privacy*: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006, p. 27; S. RODOTÀ, voce *Riservatezza,* in *Enc. it.,* VII, 2007, in *www. treccani.it*; ID., *Tecnologie e diritti,* Il Mulino, 1996, p. 55 ss.; T. TRONCHIA, *Cenni problematici sulla tutela della vita privata nell'ordinamento giuridico italiano*, Cedam, 1990, p. 148. Inizialmente, il diritto alla *privacy* viene concepito come "*right to be alone*", al fine di garantire la tutela della c.d. *inviolate personality*, ossia dell'intimità della vita domestica di ogni individuo. Sul punto, v. S.D. WARREN–L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, vol. IV, n. 5, 1890. In verità, il primo a parlare di diritto alla *privacy*, alla fine del diciannovesimo secolo, è stato il giudice Thomas Cooley, che, quasi incidentalmente, ha fatto riferimento al diritto alla riservatezza nell'ambito di uno scritto trattatistico in materia di fatti illeciti. Cfr. T.C. COOLEY, *A Treatise on the Law of Torts or the Wrongs which Arise Indipendent of contract*, Callaghan and Company, 1879, p. 29. Successivamente, il diritto alla riservatezza viene concepito come «diritto a controllare l'uso che altri fanno delle informazioni che mi riguardano». Così A. WESTIN, *Privacy and freedom*, 25 Wash. & Lee L. Rev. 166, 1968, p. 2. Secondo altri, come «proiezione delle scelte di vita contro ogni forma di controllo pubblico e di stigmatizzazione sociale». V., L.M. FRIEDMANN, *The Republic of choice. Law, authority and culture,* Harvard Univ Press, 1990, p. 4. Nonostante la teorizzazione del nuovo diritto, la giurisprudenza statunitense ne riconosce l'autonomia giuridica solo nei primi anni del 1900. Cfr. Supreme Court of the United States, Olmstead v. United States, 277 U.S. 438 (1928), in *www.supreme.justia.com*. Con questa pronuncia viene riconosciuto il diritto alla *privacy* di chi comunica privatamente per via telefonica, sul presupposto che il IV emendamento protegga non solo cose e luoghi, ma anche le persone. Nel 1974, il *Privat Act* riconosce ad ogni individuo il diritto di accedere, prendere visione e rettificare i propri dati detenuti da una *agency*. Tuttavia, numerose pronunce prevedono la protezione del diritto alla *privacy* trovandone fondamento nella Costituzione complessivamente considerata (Supreme Court of the United States, Griwold v. Cunnecticut, 381 U.S., 479 [1965] in *www.supreme.justia.com*, mentre altre nel IV emendamento (Supreme Court of the United States, Kyllo v. United States*,* 533 U.S. 27 [2001], *ivi*). Con il passare del tempo, la giurisprudenza statunitense amplia le ipotesi in cui viene garantito il riserbo, riconoscendo margini di protezione anche in luoghi diversi dal domicilio, giungendo nel tempo a ricostruire la riservatezza non solo come mero *ius excludendi alios* ma come vero e proprio diritto di controllo dei (e sui) propri dati (c.d. *control over personal information*). Cfr. United States Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S., 749 (1989).

[123] L'espressione appartiene a M. BONETTI, *Riservatezza e processo penale*, cit., p. 257.

[124] Corte EDU, Grande Camera, 2 agosto 1984, *Malone c. Regno Unito,* cit.

La *quaestio* diventa ancor più complicata allorquando il captatore informatico viene utilizzato per compiere le "altre" attività (esulanti dall'intercettazione *strictu sensu* intesa) che pur possono essere condotte una volta che il *virus* viene inoculato sulla macchina bersaglio: in questi casi, le investigazioni esplorative condotte mediante agente intrusore devono ritenersi vietate perché non presidiate da norme processuali in grado di arginare eventuali abusi[125].

4.1. *SEGUE*: LA TUTELA DELLA *PRIVACY* NEL IL DIRITTO POSITIVO

La *privacy*, quale potere di controllo dei dati personali, risulta autonoma rispetto alla riservatezza, percepita, più genericamente, come diritto di godimento della sfera individuale: come sostenuto, «[O]gnuno ha diritto alla protezione dei dati, così come ha diritto alla segretezza delle comunicazioni […]. Il trattamento dei dati va, quindi, assimilato all'intercettazione delle comunicazioni […] si tratta di due facce della stessa medaglia»[126].

In effetti, in nome dell'indipendenza di ciascuna prerogativa, i rispettivi ambiti di tutela appaiono diversificati ma complementari, nel senso che il diritto alla riservatezza trova protezione indiretta nelle norme codicistiche in tema di intercettazione[127], mentre la *privacy* nelle leggi speciali introdotte per regolamentare il c.d. trattamento dei dati personali[128].

---

[125] Sull'incostituzionalità delle attività intrusive mediante *Trojan* informatico, cfr. Cap. II, §

[126] Si esprime così L. D'ANGELO, *La conservazione dei dati del traffico*, in AA. VV., *Le nuove norme di contrasto al terrorismo*, cit., p. 131. Nello stesso senso, da ultimo, A. MANNA–M. DI FLORIO, *Riservatezza e diritto alla* privacy: *in particolare la responsabilità per omissione dell'*internet provider, in AA. VV. Cybercrime, diretto da A. Cadoppi–S. Canestrari–A. Manna–M. Papa, Utet, 2019, p. 892, per cui «[I]il diritto alla protezione dei dati personali […] è autonomo rispetto al più generale diritto alla riservatezza […]».

[127] La tutela della riservatezza in tema di intercettazioni processuali, rappresenta l'elemento fondante della nuova disciplina introdotta con la l. 103/2017. L'«ampia delega» parlamentare sembra suggerire al governo una ridefinizione della disciplina delle intercettazioni ridisegnando i confini del diritto alla riservatezza con il dichiarato intento di prevedere regole a tutela della privatezza dei soggetti (anche occasionalmente) coinvolti, senza tuttavia ridimensionare l'area operativa del mezzo di ricerca della prova, al fine ricercare un equilibrio tra l'esigenza di verità e giustizia e tutela dei diritti fondamentali. Pur senza operare un rinvio esplicito alla giurisprudenza della Corte EDU, emerge, in linea di principio, la volontà del legislatore nazionale di adeguarsi alle regole europee in materia di intercettazioni. Si pensi alla necessità di apprestare opportune cautele a protezione del diritto alla riservatezza dei soggetti anche occasionalmente coinvolti nelle intercettazioni (Corte EDU, Grande Camera, 16 febbraio 2000, *Amann c. Svizzera*, cit., § 61); alla tutela "privilegiata" delle comunicazioni tra difensore e assistito (Corte EDU, Grande Camere, 25 marzo 1998, *Kopp c. Svizzera*, cit., §§ 53 s.; sez. II, 2 dicembre 2014, *Taraneks c. Lettonia,* § 87–89); al dovere di determinare i contenuti minimi dei verbali che attestano le operazioni effettuate; alla previsione di precauzioni per assicurare l'integrità della registrazione e la distruzione dei dati captati (Corte EDU, Grande Camera, 4 dicembre 2008, *Marper c. Regno Unito*, cit., § 77; sez. I, 17 luglio 2003, *Craxi c. Italia*, cit., § 67.). Sul punto, approfonditamente, T. BENE, *Diritti e interessi coinvolti nella riforma delle intercettazioni*, in *Jus online*, 2017, p. 22 ss.; C. CONTI, *La riservatezza delle intercettazioni nella delega Orlando*, in *Dir. pen. cont.,* n. 3, 2017, p. 78 ss.; D. CURTOTTI, *Le intercettazioni nella giurisprudenza europea*, cit., p. 4 ss.; M. GIALUZ–A. CAMBIALE–J. DELLA TORRE, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. pen. cont.,* 2017, n. 3, p. 193; S. LONATI, *I criteri direttivi contenuti nella delega in materia di intercettazioni di conversazioni o comunicazioni,* in AA. VV., *Le nuove intercettazioni*, a cura di O. Mazza, Giappichelli, 2018, p. 1 ss.

[128] In dottrina, l'approccio inteso a considerare il diritto alla protezione dei dati personali quale parte integrante del diritto alla *privacy*, ovvero quale uno dei vari elementi volti a caratterizzare tale diritto (P. BLUME, *Data Protection and Privacy: Basic Concepts in a Changing World*, in *Scandinavian Studies in Law,* 2010, p. 151 ss.), è stato ormai superato dall'orientamento inteso ad individuare il diritto alla

Prima di analizzare i copiosi interventi legislativi che hanno contribuito a delineare la disciplina del diritto alla *privacy*, è opportuno chiarire il significato dei concetti–chiave su cui si fonda l'intera normativa.

Intanto, con la locuzione di "trattamento dei dati personali" «ci si riferisce ad ogni operazione o insieme di operazioni che riguarda la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la consultazione, la modificazione, l'estrazione, il raffronto, la selezione, l'utilizzazione, l'interconnessione, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati»[129].

Quanto alla nozione di "dato personale", con essa si intendono «tutte le informazioni che attengano ad una persona fisica identificata o, comunque, identificabile, [ossia quella] che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica»[130].

---

tutela delle informazioni personali quale posizione giuridica autonoma e distinta, sia pure strettamente collegata al diritto alla *privacy*. In questo senso S. RODOTÀ, "*Prefazione*", in AA. VV., *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, Giuffrè, 2006, p. VII ss.; P. DE HERT– S. GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in *Reinventing Data Protection*?, a cura di S. Gutwirth–Y. Poullet–P. De Hert–C. De Terwangne–S. Nouwt, Springer, 2009, p. 3 ss.; M. NINO, *Terrorismo internazionale,* privacy *e protezione dei dati personali,* ESI, 2012, p. 34 ss. Infatti, mentre il diritto alla *privacy*, infatti, è inteso ad evitare ingerenze arbitrarie ed ingiustificate del potere esecutivo nella riservatezza degli individui, il diritto alla protezione dei dati è volto a garantire che il trattamento delle informazioni personali individuali rispetti i principi di proporzionalità, necessità e limitazione dei dati. Quanto al contenuto, il diritto alla protezione dei dati, da un lato, presenta una più ampia portata rispetto al diritto alla *privacy*, consistendo nella attribuzione di una serie di diritti agli individui concernenti il trattamento delle informazioni personali, indipendentemente dalla circostanza che gli stessi siano ricollegabili alla *privacy*; dall'altro, esso presenta una forza espansiva molto più limitata, in quanto, mentre lo stesso concerne la sola disciplina del trattamento dei dati personali, il diritto alla *privacy* riguarda la regolamentazione e la salvaguardia di un'ampia congerie di situazioni giuridiche soggettive. Così P. HUSTINX, *EU Data Protection Law − Current State and Future Perspectives,* in *www.secure.edps.europa.eu,* p. 3. Per un quadro generale dei vari orientamenti dottrinali in materia, si veda M. BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Dir. umani e dir. internaz*., 2011, p. 437 ss., p. 440 ss. Come sostenuto, «da un canto, detti diritti sono considerati quali posizioni giuridiche soggettive coincidenti, condividendo un ampio novero di elementi strutturali (molti principi ispiratori del diritto alla *privacy* orientano, difatti, la disciplina del trattamento delle informazioni di carattere personale); d'altro canto, gli stessi presentano, ciascuno, caratteristiche proprie, distinguendosi tanto per finalità quanto per contenuto. Peraltro, tali diritti, pur essendo espressione di categorie soggettive autonome, presentano forti analogie tra di loro, essendo in grado di sovrapporsi in molte situazioni in cui vengono in rilievo, ed essendo molto più simili che diversi». Si esprime così M. NINO, *Il caso* Datagate: *i problemi di compatibilità del programma di sorveglianza* PRISM *con la* nrmativa europea sulla protezione dei dati personali e *della* privacy, cit., p. 728.

[129] Così art. 1 comma 2, lett. *b*, l. 675/1996. Sulla nozione *de qua*, più di recente, S. SIGNORATO, *Il trattamento dei dati personali per fini di polizia*, in AA. VV., *Il nuovo "pacchetto" antiterrorismo,* a cura di R.E. Kostoris–F. Viganò, Giappichelli, 2015, p. 92. Si deve, tuttavia, precisare, che un trattamento dei dati può essere effettuato per le più diverse finalità, quali quelle commerciali, sanitarie, statistiche, di polizia. Per quel che in questa sede rileva, l'attenzione sarà focalizzata solo in relazione al trattamento dei dati personali a fini di polizia, sia per l'accertamento che per la prevenzione dei reati.

[130] Così art. 3, n. 1 della Direttiva (Ue) 2016/680 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

Un aspetto particolare del trattamento dei dati personali, inerisce alla "conservazione dei dati del traffico telefonico o telematico"[131] (c.d. *data retention*) che «può addirittura essere più "pericolosa" dal momento che […] consente di rivolgere anche uno sguardo al passato. È, allora, facile da percepire che la sfera di tutela del diritto alla protezione dei dati è direttamente proporzionate alle regole adottate, in un particolare momento storico, per determinare la lunghezza del tempo di conservazione dei dati»[132].

Questo è il motivo per cui, come meglio si vedrà di seguito, il legislatore si mostra particolarmente attento alla tematica *de qua*, modificando di volta in volta i termini di conservazione dei dati, tentando di adeguarsi agli orientamenti internazionali[133].

Ritornando alla genesi normativa del diritto, va detto che la tutela della *privacy*, soprattutto grazie alle spinte europeiste in materia[134], trova una disciplina organica, sia pur limitata alla «tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali», nella l. 675/1996[135].

Nel testo, tuttavia, nulla si dice in relazione alla conservazione dei dati: così, al fine di supplire alla lacuna or ora evidenziata, il legislatore, a soli due anni distanza, interviene sulla

---

[131] Per "dato relativo al traffico", si intende «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione». Così art. 4 comma 2, lett. *h*, d.lgs. 193/2003 (Cod. *privacy*). Sul significato da attribuire alla locuzione *de qua*, AA. VV., *Codice in materia di protezione dei dati personali,* a cura di G. Cassano–S. Fadda, Ipsoa, 2004, p. 570 ss.; L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 155 ss.; A. MONTI, *Decreto legislativo 196/03: il senso delle parole*, in *www.interlex.it;* ID., *Decreto legislativo 196/03: l'internet non è una rete*, *ivi*.

[132] Si esprime così L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 132.

[133] Come sostenuto, le costanti modifica alla disciplina del trattamento dei dati, testimonia «[…] la difficoltà a trovare il giusto equilibrio in una materia in cui sia le esigenze sociali sottese alle leggi che le tecniche dell'attività di trattamento dei dati sono in continuo divenire». Così L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 138.

[134] Si pensi, a titolo meramente esemplificativo, alla Direttiva 95/46/CE, del Parlamento europeo e del Consiglio del 23 novembre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di essi, del 23 novembre 1995; alla Direttiva 97/66/CE, del Parlamento europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni ha avuto il compito di tradurre i principi della citata direttiva in norme specifiche per il settore delle telecomunicazioni, del 30 gennaio 1998; alla direttiva 2006/24/CE, del Parlamento europeo e del Consiglio, del 13 aprile 2006 (cd. direttiva "*data retention")*, riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. Per un commento, esaustivamente, C. CONTI, *L'attuazione della direttiva Frattini: un bilanciamento insoddisfacente tra riservatezza e diritto alla prova*, in AA. VV., *Le nuove norme sulla sicurezza pubblica*, a cura di S. Lorusso, Cedam, 2008, p. 3 ss. Va precisato che, di recente, la Corte EDU ha dichiarato invalida la direttiva 2006/24/CE, su cui si rinvia a nt. 185.

[135] L. 31 dicembre 1996, n. 675, recante "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"*, in *Gazz. uff.,* 8 gennaio 1997, n. 5, in *www.garanteprivacy.it*. In argomento, C.M. BIANCA–F.D. BUSINELLI, *Tutela della* privacy, in *Nuove l. civ. comm*., 1999, p. 219 s.; G. BUTTARELLI, *Banche dati e tutela* della riservatezza, Giuffrè, 1997; V. CUFFARO–V. RICCIUTO, *La disciplina del trattamento dei dati personali,* Giappichelli, 1997; V. DENTI, *La tutela della riservatezza: profili processuali*, in *Riv. trim. dir. e proc. civ*., 1998, p. 747 ss.; R. GALBIATI, *Autorità garanti. Profili processuali*, in *Foro it*., 1998, f. 1, p. 43 ss.; E. GIANNANTONIO–M.G. LOSANO–M.G. ZENO ZENCOVICH, *La tutela dei dati personali: commentario alla legge 675 del 1996*, Cedam, 1997; A. ORESTANO, *La riservatezza ancora una volta in* Cassazione: fondamento, contenuto e *limiti all'indomani dell'entrata in vigore della l. n. 675/96,* in *Danno e responsabilità*, 1998, p. 865.

materia, disponendo che tutti i dati – senza alcuna distinzione tra telefonici e telematici – debbano essere «cancellati o resi anonimi al termine della chiamata»[136].

Pur non sussistendo alcun obbligo di conservazione dei dati personali del traffico per scopi investigativi di prevenzione o accertamento dei reati, nella prassi le società di telecomunicazione e gli *internet service provider*, in spregio alle norme di diritto positivo, garantiscono la conservazione degli stessi per una durata massima di cinque anni; nel contempo, l'autorità giudiziaria, in assenza di espressa disciplina in materia e richiamando le regole generali del codice di rito[137], acquisisce «senza problemi»[138] ogni informazione utile per le proprie indagini.

L'ambiguità della disciplina, combinata ad una prassi non incline all'interpretazione rigorose della – seppur scarna – normativa, impone al legislatore un ulteriore intervento.

Con lo scopo di dotare la materia in esame di regole più rispettose dei principi fondamentali e, al contempo, maggiormente in grado di soddisfare le esigenze investigative, l'intera disciplina in materia di protezione dei dati viene raccolta in un unico *corpus* legislativo (c.d. Codice *privacy*)[139], in cui viene nettamente distinta la normativa inerente al trattamento dei dati personali per scopi di polizia (art. 53 Cod. *privacy*)[140] da quella riguardante la conservazione dei dati del traffico telefonico e telematico (art. 132 Cod. *privacy*)[141].

---

[136] Ai sensi dell'art. 4, d.lgs. 13 maggio 1998, n. 171, recante "*Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica*", in *www.garanteprivacy.it*. Alla regola *de qua* fanno, tuttavia, eccezione i dati necessari per le finalità di fatturazione, da conservare per un periodo massimo di cinque anni, secondo quanto previsto dall'art. 2948, n. 4 c.c.

[137] Ai sensi degli artt. 248 (Richiesta di consegna) e 256 (Dovere di esibizione e segreti) c.p.p.

[138] Così L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 139

[139] D. lgs. 30 giugno 2003, n. 196, recante "*Codice in materia di protezione dei dati personali*", in *Gazz. uff*., 29 luglio 2003, n. 174, in *www.camera.it*. Per commenti, *ex multis*, AA. VV., *Codice in materia di protezione dei dati personali,* cit.; R. ARNABOLDI, *Codice della* privacy *e DPS. Flussi processuali*, Giuffrè, 2010, p. 81 s.; M. DE GIORGI–A. LISI, *Guida* al *Codice della* privacy. *La protezione dei dati personali alla luce del d.lgs. 196/2003*, Edizioni Giuridiche Simone, 2003; G. ELLI–L. ZALLONE, *Il nuovo Codice della* privacy *con la giurisprudenza del Garante*, Giappichelli, 2004; S. FRAUTACIELLO, *La protezione dei dati personali come limite all'accertamento penale*, in AA. VV., *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?,* cit., p. 117 ss.

[140] Ai sensi dell'art. 53 Cod. *privacy*, «[N]non si applicano le seguenti disposizioni del Codice al trattamento di dati personali effettuato dal C.e.d. del dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o da altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica , prevenzione, accertamento o repressione dei reati , effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento: art. 9 (modalità di esercizio dei diritti interessati); art. 10 (riscontro dell'interessato); art. 12 (codici di deontologia e nuova condotta); art. 13 (informativa); art. 16 (cessazione del trattamento); artt. da 18 a 22 (regole specifiche per i soggetti pubblici); artt. 39–45 (obbligo di comunicazione e regole per il trasferimento dei dati all'estero); artt. da 145 a 151 (tutela dinanzi al Garante)». Per commenti, R. ARNABOLDI, *Codice della* privacy *e DPS. Flussi processuali*, cit., p. 81 s.; R. BORRELLO, *Il trattamento dei dati personali da parte delle Forze di Polizia*, in AA. VV., *Attività delle forze di polizia e trattamento dei dati personali*, Maggioli editore, 2012, p. 61 ss.; S. FRAUTACIELLO, *La protezione dei dati personali come limite all'accertamento penale*, cit., p. 123 ss.

[141] Nella formulazione prevista, l'art. 132 Cod. *privacy* prescrive che i dati relativi al traffico telefonico devono essere conservati dal fornitore, per un periodo non superiore a trenta mesi, «secondo le modalità individuate con decreto del Ministro della giustizia, di concerto con i Ministri dell'interno e delle comunicazioni, e su conforme parere del Garante». Come si evince dal dettato normativo, nell'ottica del bilanciamento tra efficacia delle indagini e protezione del diritto alla *privacy*, il legislatore del 2003 propende per il secondo. Si è detto, infatti, che «[S]si trattava di una soluzione che offrire ampi margini di tutela alla *privacy* degli utenti, ma suscitava molte perplessità sul piano

Per quanto concerne la prima, va detto che la normativa relativa al trattamento dei dati per scopi di polizia subisce ulteriori "rimaneggiamenti": infatti, l'art. 7 del d.l. 7/2015, così come modificato dalla legge di conversione 43/2015[142], sostituisce integralmente il contenuto dell'art. 53 Cod. *privacy*.

Intanto la novella, colmando la lacuna dell'originaria formulazione, chiarisce la portata della condizione legittimante il trattamento dei dati personali: in particolare, la "finalità di polizia" ricorre allorquando i trattamenti dei dati personali risultino «direttamente correlati all'esercizio dei compiti di polizia, di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati»[143].

Il d.p.R 15/2018, all'art. 8, comma 1, introduce una specifica disciplina inerente all'utilizzo dei sistemi di videosorveglianza, di ripresa fotografica, video e audio: ribadendo il divieto di ingerenza ingiustificata nelle libertà fondamentali individuali[144], viene consentita l'attività *de quibus* per le finalità di polizia giudiziaria, per la difesa dell'ordine e della sicurezza pubblica o della vita umana[145], con il duplice limite di raccogliere solo i dati strettamente necessari per le investigazioni[146] e di adottare misure tecnologiche che assicurino la riservatezza dei dati, ne minimizzino il rischio di distruzione o di accesso abusivo [147].

---

dell'efficacia investigativa, soprattutto perché nulla prevedeva per le comunicazioni via internet». L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 144.

[142] D.l. 18 febbraio 2015, n. 7, in *Gazz. uff*., 19 febbraio 2015, n. 41, convertito, con modificazioni, dalla l. 17 aprile 2015, n. 43, recante "*Conversione in legge, con modificazioni, del decreto–legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo, anche di matrice internazionale, nonchè proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle Organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazion"e*, in *Gazz. uff*., 20 aprile 2015, n. 91, cfr. *www.gazzettaufficiale.it*.

[143] Ai sensi del novellato art. 53, comma 1 Cod. *privacy*.

[144] *Ex* art. 22, d.p.R. 15/2018, inerente ai "*Sistemi di videosorveglianza*", «[L]l'utilizzo di sistemi di videosorveglianza è consentito ove necessario per le finalità di polizia […] e a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate. Gli organi, uffici e comandi di polizia, […] raccolgono solo i dati strettamente necessari per il raggiungimento delle [suddette] finalità, […] registrando esclusivamente le immagini indispensabili».

[145] L'art. 3, d.p.R. 15/2018, relativo alla "*Finalità dei trattamenti*", definisce l'ambito applicativo dell'attività *de qua*. In particolare, per «[…] finalità di polizia, ai sensi dell'articolo 53 del Codice, quando sono direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati […]». Inoltre, l'art. 23, d.p.R. 15/2018, precisa che «[L]l''utilizzo di sistemi di ripresa fotografica, video e audio per le finalità di polizia di cui all'articolo 3, è consentito ove necessario per documentare: una specifica attività preventiva o repressiva di fatti di reato, situazioni dalle quali possano derivare minacce per l'ordine e la sicurezza pubblica o un pericolo per la vita e l'incolumità dell'operatore, o specifiche attività poste in essere durante il servizio che siano espressione di poteri autoritativi degli organi, uffici e comandi di polizia».

[146] Ai sensi del comma 2 dell'art. 24 comma 2, d.p.R. 15/2018, recante "*Speciali misure di sicurezza relative al trattamento di dati attraverso sistemi di videosorveglianza e di ripresa fotografica, audio e video"*, «[G]gli organi, uffici e comandi di polizia, nel rispetto dei principi richiamati dagli articoli 4, 5 e 6, raccolgono solo i dati strettamente necessari per il raggiungimento delle finalità di polizia di cui all'articolo 3, registrando quelli indispensabili».

[147] L'art. 25, d.p.R. 15/2018, rubricato "*Obblighi di sicurezza*", sancisce che: «[I]il titolare o il responsabile del trattamento dei dati personali assicurano l'adozione di misure di sicurezza preventive, individuate anche in relazione al progresso tecnologico, alla natura dei dati e alle caratteristiche del singolo trattamento, idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di cui all'articolo 3 ed a garantirne, nel contempo, un'agevole fruibilità».

Da ultimo, nel *mare magnum* delle riforme legislative sul tema, stiamo assistendo a quella che può essere definita la più ingente modifica normativa della disciplina del trattamento dei dati personali, mossa dalla duplice necessità di adeguare la protezione dei dati all'evoluzione tecnologica e, al contempo, garantire l'uniforme circolazione degli stessi nell'ambito dell'Unione[148].

[148] Si tratta del c.d. "Pacchetto Protezione dei dati UE", comprendente il Regolamento europeo 2016/679 (GDPR, *General Data Protection Regulation*), relativo alla "*Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*", entrato in vigore il 24 maggio 2016 e divenuto definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018 e la Direttiva 2016/680, relativa alla "*Regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione di sanzioni penali*", entrata in vigore il 5 maggio 2016 e recepita dai Paesi UE entro 2 anni dall'entrata in vigore. Più nel dettaglio, con il GDPR si tende a «contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche», in quanto «[L]la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. […] La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione […]». Così Regolamento (UE) 2016/679, considerando nn. 2 e 6. Secondo quanto disposto dall'art. 2 del Regolamento, lo stesso non si applica ai trattamenti dei dati personali «effettuati dalle autorità competenti ai fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e alla prevenzione delle stesse», in quanto oggetto di una specifica disciplina da parte della direttiva (UE) 2016/680. Sul punto, G. SCORZA, sub *art. 2*, in AA. VV., *GDPR e normativa* privacy. *Commentario*, a cura di G.M. Riccio–G. Scorza–E. Belisario, Wolters Kluwer, 2018. La direttiva, raccogliendo gli auspici del Consiglio Europeo, come formulati nel Programma di Stoccolma, in *Gazz. Uff. CE*, C 115, 4 maggio 2010, n. 1, sorge dall'esigenza avvertita nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, di stabilire norme specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. Infatti, «[È] è […] opportuno per i settori in questione che una direttiva stabilisca le norme specifiche relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività […]». Così Direttiva (UE) 2016/680, Considerando n. 11. In passato, la disciplina della protezione dei dati personali è stata affidata alla Convenzione n. 108/1981 del Consiglio d'Europa, adottata a Strasburgo il 28 gennaio del 1981, e alla Raccomandazione adottata dal Comitato dei ministri il 17 settembre 1987 R (87) 15, relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza. Un quadro generale per la protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia si è avuto solo nel 2008 con l'adozione della Decisione quadro 2008/977/GAI, in *Gazz. Uff. CE*, L 350, 30 dicembre 2008, n. 60. Sul tema, diffusamente, L. PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri reati gravi*, in *Proc. pen. e giust*., 2018, f. 6, p. 1139 ss.; P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, in AA. VV., *La nuova disciplina europea della* privacy, a cura di S. Sica–V. D'Antonio–G.M. Riccio, Cedam, 2016, p. 325. Sul tema già G. TIBERI, *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in AA. VV., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, a cura di G. Grasso–L. Picotti–R. Sicurella, Giuffrè, 2011, p. 515, che sostiene che la direttiva è contraddistinta da numerose lacune e «rischia di essere uno strumento già vecchio e inadeguato ad affrontare i problemi che emergono dai nuovi metodi di lavoro che si sono ormai imposti nell'attività di contrasto al terrorismo e alla criminalità, alimentati dagli sviluppi tecnologici degli ultimi anni e dalla richiesta sempre maggiore di dati personali per affrontare le nuove sfide». In questo contesto,

In quest'ottica, il legislatore delegato approva il d.lgs. 51/2018 in materia di trattamento e circolazione dei dati personali per finalità di polizia[149], introducendo nuove regole per

sembra che il legislatore europeo abbia voluto innalzare il livello di sicurezza collettivo, anche con il rischio, non per altro peregrino, di determinare un *vulnus* per i diritti individuali. Infatti, nel testo si legge che «[N]nell'interesse della prevenzione, dell'indagine e del perseguimento di reati, è necessario che le autorità competenti trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto per sviluppare conoscenze delle attività criminali e mettere in collegamento i diversi reati accertati. Per mantenere la sicurezza relativamente al trattamento e prevenire trattamenti che violano la presente direttiva, i dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche impedendo l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento, e da tenere conto dello stato dell'arte e della tecnologia disponibili, dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere». Così Direttiva (UE) 2016/680, Considerando n. 27 e 28. Inoltre, «[I]il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, dovrebbe riguardare qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali per tali finalità, con l'ausilio di strumenti automatizzati o in altro modo, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione del trattamento, la cancellazione o la distruzione». Così Direttiva (UE) 2016/680, Considerando n. 34. Per dovere di completezza si segnale che Regolamento (UE) 2016/679 viene recepito con d.lgs. 101/2018. Sul punto, si rinvia a nt. 150. Sui lavori di attuazione e per un inquadramento dei due decreti attuativi, D. CERTOSINO, De jure condendo*,* in *Proc. pen. giust.,* 2018, f. 1, p. 463; C. PANSINI, *Novità legislative*, *ivi,* 2018, f. 2, p. 690. Più in generale, sull'*iter* di riforma, AA. VV., *La riforma della* privacy. *Guida pratica per l'applicazione del nuovo Regolamento europeo (Gdpr),* a cura di A. Ciccia Messina, Italia Oggi, 14 marzo 2018; AA. VV., *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679,* a cura di L. Califano–C. Colapietro, Editoriale Scientifica, 2017; G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA. VV., Cybercrime, cit., p. 1599 ss.; M. BASSINI, *La svolta della* privacy *europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quad. cost.*, 2016, p. 587 ss.; C. DI FRANCESCO, *Maesa, Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*, in *Eurojus*.it, 24 maggio 2016; F. DI RESTA, *La nuova* "privacy *europea". I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori*, Giappichelli, 2018; D. LABIANCA, *Il sistema delle tutele nel regolamento europeo n. 679/2016 sulla protezione dei dati personali*, in AA. VV., Cybercrime, cit., p. 978 ss.; E. PELINO–C. BISTOLFI–L. BOLOGNINI, *Il Regolamento europeo. Commentario alla nuova disciplina sulla protezione dei dati,* Milano, 2016; S. GORLA–C. PONTI, Privacy *UE. Il vecchio e il nuovo: confronto tra d.lgs 196/2003 Codice* privacy *e Regolamento 2016/679 Gdpr,* Iter, 2018; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli, 2018, p. 37 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 87 ss.; P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., p. 319 ss.

[149] D.lgs. 18 maggio 2018, n. 51, recante "*Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonchè alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio*", in *Gazz. uff.,* 24 maggio 2015, n. 119, cfr. *www.gazzettaufficiale.it.* Si tratta di un testo unitario, dedicato alla complessiva disciplina del trattamento di dati personali con l'obiettivo di creare un vero e proprio statuto, contenente principi generali di regolamentazione della materia e disposizioni di dettaglio nei vari settori in cui si può articolare il trattamento dei dati personali. In tema S. CARRIER, Privacy *e diritto penale: approvato in via definitiva il d. lgs. 51/2018 che attua la direttiva europea sulla tutela dei dati personali a fini di pubblica sicurezza e penali*, in *Giur. pen.* web, 2018, f. 5, p. 1 ss.;

l'acquisizione di ogni dato utile alle investigazioni. Più nel dettaglio, l'art. 47 della novella attribuisce alle autorità alle Forze di polizia il potere di acquisire informazioni, atti e documenti da altri soggetti, anche per via telematica, avvalendosi di convenzioni tese ad agevolarne la consultazione tramite reti di comunicazione elettronica, pubblici registri, elenchi, schedari e banche dati[150].

Ancor più complesso è l'*iter* legislativo inerente alla c.d. *data retention*, ossia il regime di conservazione dei dati relativi al traffico telefonico e telematico, per cui, a partire dalla legislazione del 2003, si innesca un effetto domino che importa ben nove interventi successivi di assestamento normativo[151].

A. CISTERNA*, Il difficile equilibrio tra sicurezza interna e tutela dei diritti*, in *Guida dir*., 2018, *Dossier* n. 3, p. 81 ss.; A. DI TULLIO D'ELISIIS, *Nuovi illeciti penali introdotti dal decreto legislativo n. 51/2018*, in *www.diritto.it*, 6 giugno 2018; G. NAZZARO, *La* privacy *in ambito penale. Ecco il nuovo statuto*, in *Sic. e giust.,* n. N. II_MMXVIII; L. PULITO, *Il trattamento dei dati personali in ambito penale e l'uso del* passenger name record *per contrastare il terrorismo e altri reati gravi*, cit., 1141 ss.; F. SORRENTINO, *Il controllo del garante per la protezione dei dati personali e l'autorità giudiziaria secondo le più recenti norme eurounitarie*, in *www.questionegiustizia.it*, 15 febbraio 2018. Da ultimo, G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati,* cit., p. 1599 ss.; M. TORRE, Privacy *e indagini penali*, cit., p. 30 ss.

[150] Art. 47, d.lgs. 51/2018, rubricato "*Modalità di trattamento e flussi di dati da parte delle Forze di polizia*", ai sensi del quale, «[N] Nei casi in cui le autorità di pubblica sicurezza o le Forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli da 3 a 8. […]. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati […]. I dati trattati dalle Forze di polizia per le finalità di cui all'articolo 1, comma 2, sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo. […]».

[151] La disciplina delineata dal d.lgs. 196/2003, a pochi mesi dalla sua prima formulazione, viene integralmente sostituita dal d.l. 24 dicembre 2003, n. 354, recante "*Disposizioni urgenti per il funzionamento dei tribunali delle acque nonché per l'amministrazione della giustizia*", cfr. *www.gazzettaufficale.it.* Il nuovo testo contempla, dopo i trenta mesi previsti per l'accertamento e la repressione di tutti i reati, un ulteriore periodo di conservazione di trenta mesi, destinato esclusivamente alle investigazioni per gravi delitti; inoltre estende l'operatività del meccanismo di conservazione ai dati provenienti da ogni tipo di comunicazione, equiparando il traffico telematico a quello telefonico. A seguito dei plausibili malcontenti della società civile e degli *internet provider* – nonché della dura presa di posizione del Garante per la *privacy* (Cfr. Comunicato stampa del 23 dicembre 2003, in *www.garanteprivacy.it)* – la norma subisce ulteriori modifiche. Tra queste, la l. 26 febbraio 2004, n. 45, recante "*Conversione in legge, con modificazioni, del decreto–legge 24 dicembre 2003, n. 354, recante disposizioni urgenti per il funzionamento dei tribunali delle acque, nonché interventi per l'amministrazione della giustizia*", in *Gazz. uff*., 27 febbraio 2004, n. 48, cfr. *www.gazzettaufficale.it,* in cui all'art. 3, si introducono evidenti modifiche al testo dell'art. 132 Codice *privacy* in termini di durata dei termini di conservazione (ventiquattro mesi, prorogabili di altri ventiquattro nel caso di delitti di cui all'art. 407 comma 2, lett. *a*, c.p.p.); il d.l. 27 luglio 2005, n. 144, recante "*Misure urgenti per il contrasto del terrorismo internazionale*", in *Gazz. uff.,* 27 luglio 2005, n. 173, convertito, con modificazioni in l. 31 luglio 2005, n. 155, recante "*Misure urgenti per il contrasto del terrorismo internazionale*", in *Gazz. uff.,* 1 agosto 2005, n. 177, cfr. *www.camera.it,* con cui (*ex* art. 6 comma 3, l. 177/2005) si introducono nuove norme sui dati del traffico telefonico e telematico, incidendo sui termini e sull'elenco dei dati da conservare, sulle modalità di identificazione degli intestatari delle utenze telefoniche, sulle procedure per l'acquisizione degli elementi esterni dalle comunicazioni agli atti del processo penale. Più tardi, l'art. 132 Cod. *privacy* viene ulteriormente modificato dall'art. 2 comma 1 del d.lgs. 30 maggio 2008, n. 109, attuativo della

Allo stato dell'arte, la legge europea 2017[152] prevede che gli operatori telefonici, in rapporto all'accertamento ed alla repressione dei delitti consumati o tentati con finalità di terrorismo (art. 51, comma 3 *quater* c.p.p.) e dei reati ricompresi nell'elenco fissato all'art. 407, comma 2 lett. *a* c.p.p.[153], siano tenuti a conservare i dati del traffico telefonico e telematico, nonché quelli relativi

direttiva 2006/24/CE (poi dichiarata invalida nel 2014 da CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland e Seitlinger,* cause riunite C–293/12 e C–595/12, in *Giur. it.,* 2014. Si prevede che, per finalità di accertamento e repressione dei reati, i dati relativi al traffico telefonico devono essere conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, mentre i dati che attengono al traffico telematico vanno conservati, sempre dal fornitore e in vista delle medesime finalità, per dodici mesi. Il comma 1 *bis* stabilisce, inoltre, che i dati relativi alle chiamate senza risposta devono essere conservati per trenta giorni. Per un'analisi di tali provvedimenti, F. CERQUA, *Il difficile equilibrio tra la protezione dei dati personali e le indagini informatiche*, in AA. VV., *Sistema penale e criminalità informatica. Profili sostanziali e processuali nella Legge attuativa della Convenzione di Budapest sul cybercrime (l. 18 marzo 2008, n. 48)*, Giuffrè, 2009, p. 221 ss.; L. D'ANGELO, *La conservazione dei dati del traffico*, cit., p. 131 ss.; A. STRACUZZI, Data retention: *il faticoso percorso dell'art. 132 Codice* privacy *nella disciplina della conservazione dei dati di traffico*, in *Dir. informazione e informatica*, 2008, f. 4–5, p. 585 ss.; G. VACIAGO, *La disciplina normativa sulla* data retention, in AA. VV., Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di L. Luparia, Giuffrè, 2012, p. 143 ss. Inoltre, l'art. 4 *bis* del d.l. 18 febbraio 2015, n. 7, escludendo la possibilità di conservare i contenuti delle comunicazioni telematiche, prevede che i dati relativi al traffico telefonico e telematico «effettuato a decorrere dalla data di entrata in vigore della legge di conversione [del d.l. 7/2015] sono conservati dal fornitore fino al 31 dicembre 2016 per finalità di accertamento e repressione dei reati». Un'identica disciplina viene fissata per i dati relativi alle chiamate senza risposta che siano trattati temporaneamente da parte dei fornitori dei servizi di comunicazione elettronica accessibile al pubblico oppure di una rete pubblica di comunicazione. Si prevede, inoltre, che in entrambi i casi, le relative disposizioni cessano di applicarsi dal 1 gennaio 2017. Sul punto, *amplius*, S. SIGNORATO, *Contrasto al terrorismo e* data retention: *molte ombre e poche luci*, in AA. VV., *Il nuovo "pacchetto" antiterrorismo*, cit., p. 75 ss.

[152] Legge 20 novembre 2017, n. 167, recante "*Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea*". Trattasi di una legge europea approvata con la finalità di contrasto e prevenzione della criminalità e di lotta al terrorismo e, a tale riguardo, viene indicato espressamente un "ancoraggio" comunitario nell'art. 20 della Direttiva UE 2017/541, ai sensi del quale gli Stati Membri adottano le misure necessarie per assicurare efficaci strumenti per l'indagine e l'esercizio dell'azione penale contro i reati legati al terrorismo.

[153] Come precisato, «[D]da una lettura sinergica delle discipline fissate dall'art. 132 Codice *privacy* e dall'art. 24 legge europea, si potrebbe pensare che il quadro complessivo della disciplina in tema di *data retention* si moduli in una sorta di doppio binario a seconda del tipo di reato perseguito. Da un lato, i tempi di conservazione sarebbero di regola scanditi nelle tempistiche di ventiquattro mesi, dodici mesi, trenta giorni previste dall'art. 132 Codice *privacy*. Dall'altro, nei casi in cui vengano in rilievo reati a matrice terroristica o previsti dall'art. 407 comma 2 lett. a, i tempi di conservazione sarebbero dettati dalla legge europea 2017 e, quindi, coinciderebbero in settantadue mesi». Così S. SIGNORATO, *Novità in tema di* data retention. *La riformulazione dell'art. 132 Codice* privacy *da parte del d.lgs. 10 agosto 2018, n. 101,* in *Dir. pen. cont.,* f. 11, 2018, p. 156.

alle chiamate senza risposta, per il termine di 72 mesi[154], estendendo in maniera significativa le tempistiche previste dal 2 comma 1 del d.lgs. 30 maggio 2008, n. 109[155].

La conseguenza è tutt'altro che di scarsa rilevanza. L'entrata in vigore della legge europea 2017 erode l'applicabilità dell'art. 132, comma 1 ed 1 *bis,* Codice *privacy* per la parte in cui esso fissa le tempistiche di conservazione dei dati, di modo che «[L]a disciplina emergenziale stabilita per il terrorismo [finisca per] divenire disciplina ordinaria»[156].

Da ultimo, il d.p.R. 15/2018 introduce una disciplina *ad hoc* in relazione ai termini di conservazione dei dati trattati dalle Forze di polizia per la prevenzione e la repressione dei reati[157].

In base ad un articolato sistema che differenzia i tempi di conservazione in ragione del tipo di provvedimento adottato, l'art. 10 del d.p.R. 15/2018, al comma 4, prevede che tali termini debbano essere aumentati allorquando i dati personali sono trattati nell'ambito di attività di prevenzione o repressione relative ai delitti di cui all'art. 51, commi 3 *bis*, 3 *quater* e 3 *quinquies*, nonché per le ulteriori ipotesi indicate dall'art. 407, comma 2, lett. *a*, c.p.p.

Tuttavia, peculiari cautele vengono poste in essere al fine di evitare la conservazione *sine die* delle informazioni apprese: i nuovi sistemi informativi e programmi informatici, infatti, devono essere progettati in modo tale che i dati personali vengano cancellati o resi anonimi, con modalità automatizzate, allo scadere dei termini di conservazione previste e in modo da consentire la documentazione in appositi registri degli accessi e delle operazioni effettuati dai soggetti abilitati.

In questo magmatico settore, la possibilità di acquisire, trattare e conservare per lunghi periodi temporali i dati appresi per finalità di polizia, finisce per rappresentare il principale *punctum dolens* della disciplina delle intercettazioni. Pericolo che risulta assai più concreto nel

---

[154] La disciplina è fatta salva dal nuovo d.lgs. 101/2018, di recepimento del Regolamento 2016/679. In particolare, l'art. 11, d.lgs. 101/2018 interviene sull'art. 132 Codice *privacy*, inserendo, tra l'altro, un nuovo comma 5 *bis*, ai sensi del quale «è fatta salva la disciplina di cui all'art. 24 della l. 20 novembre 2017, n. 167». Cfr. D.lgs. 10 agosto 2018, n. 101, recante "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*". Per commenti, AA. VV., *Il processo di adeguamento al GDPR*, a cura di G. Cassano–V. Colarocco, Giuffrè, 2018; V. CUFFARO, *Quel che resta di un codice: il D.Lgs. 10 agosto 2018, n. 101 detta le disposizioni di adeguamento del codice della privacy al regolamento sulla protezione dei dati*, in *Corr. Merito*, 2018, f. 10, p. 1108 ss. F. SARZANA, *Gdpr, la* privacy *europea è in vigore da oggi. Ma ognuno la applica a modo suo,* cfr. *www.ilfattoquotidiano.it,* 4 settembre 2018; S. SIGNORATO, *Novità in tema di* data retention. *La riformulazione dell'art. 132* Codice privacy *da parte del d.lgs. 10 agosto 2018, n. 101,* cit., p. 153 ss. Da ultimo, M. BACCARI, *Il trattamento (anche elettronico) dei dati personali,* cit., p. 1599 ss.

[155] La novella suscita dubbi e perplessità in ragione della presunta incompatibilità della disciplina de qua con i dettami europei che impongono regole assai più stringenti, rispettose del principio di proporzionalità. Cfr. Corte EDU, Grande Camera, 4 dicembre 2008, *Marper c. Regno Unito*, cit., nonché CGUE, Grande Sezione, 21 dicembre 2016, *Tele2 e Watson*, cause riunite C–203/15 e C–698/15. Ma già, CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland e Seitlinger,* cause C–293/12 e C–594/12, §45 ss., cit. Come sostenuto, la norma è un *unicum* nell'Unione europea e anche per questo motivo ha espresso la sua contrarietà il Garante *privacy,* Antonello Soro, secondo cui: *«[S]se la minaccia di attacchi informatici è quotidiana, diventa ancora più incomprensibile la decisione di aumentare fino a 6 anni la Data Retention, ignorando, non solo le sentenze della Corte di giustizia europea e della Corte EDU, ma anche il buon senso». Così A. SORO,* Convegno *Privacy digitale e protezione dei dati personali tra persona e mercato svoltosi a Firenze*, 24 ottobre 2018. Sul punto, cfr. S. SIGNORATO, *Novità in tema di* data retention. *La riformulazione dell'art. 132* Codice privacy *da parte del d.lgs. 10 agosto 2018, n. 101,* cit., p. 156.

[156] S. SIGNORATO, *Novità in tema di* data retention. *La riformulazione dell'art. 132 Codice* privacy *da parte del d.lgs. 10 agosto 2018, n. 101,* cit., p. 157.

[157] Cfr. D.P.R. 15 gennaio 2018, n. 15, cit.

caso di captazioni condotte mediante *virus* informatico, per cui la mole di dati appresi risulta assai più conspicua rispetto a quella ottenibile dall'esecuzione delle tradizionali intercettazioni, acuendo il rischio di un'indebita circolazione di informazioni tra diversi procedimenti e favorendo la canalizzazione dei dati ottenuti *ultra vis* quale *escamotage* per intentare – impropriamente – un nuovo *iter* processuale[158].

5. L'INNOVAZIONE TECNOLOGICA E I DIRITTI DI "TERZA GENERAZIONE". DAL DOMICILIO INFORMATICO AL DIRITTO ALL'INTANGIBILITÀ DELLA VITA DIGITALE

La "rivoluzione tecnologica" dell'ultimo ventennio dirama i suoi effetti non solo sulle modalità attuative delle prerogative individuali ma anche sul loro stesso contenuto, «al punto da richiedere sia l'elaborazione di diritti nuovi sia la configurazione di inedite declinazioni dei diritti tradizionali, il cui riconoscimento è ancora in divenire»[159]. Inoltre, l'avvento della ICT (*Information and Communication Technologies*) rende sempre meno distinguibile il confine tra la violazione dell'uno o dell'altro diritto, favorendo piuttosto una contemporanea trasgressione di più precetti. Si pensi ai c.d. *computer crimes* che determinano la violazione dello spazio virtuale utilizzato da un sistema informatico[160]: contenendo lo stesso una mole di dati concernenti la vita

---

[158] Cap. V, §?.

[159] Si esprime così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 49. Circa l'incidenza dello sviluppo scientifico e tecnologico nel processo penale, significativamente, F. STELLA, *Giustizia e modernità. La tutela dell'innocente e la protezione delle vittime*, Giuffrè, 2003, p. 3 ss. Sul tema anche D. CURTOTTI–L. SARAVO, *Il volo di Icaro delle investigazioni sulla scena del crimine: il ruolo della polizia giudiziaria*, in AA.VV., *Scienza e processo penale. Nuove frontiere e vecchi pregiudizi,* a cura di C. Conti, Giuffrè, 2011; G. FIANDACA, *Il giudice di fronte alle controversie tecnico–scientifiche. Il diritto e il processo penale*, in *Diritto & questioni pubbliche*, 2005, f. 5, p. 7; R. FLOR, voce *Riservatezza informatica*, in *Dir.* on line, Treccani*,* 2017; ID., *Nuove tecnologie e giustizia penale in Europa tra esigenze di accertamento e prevenzione dei reati e* quelle di tutela della *riservatezza: il ruolo "propulsore" della Corte di Giustizia*, in *Studi in onore di Maurizio Pedrazza,* cit., p. 247 ss.; ID., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in *Dir. pen. cont.,* 22 settembre 2012; L. LUPARIA, *Progresso penale e tecnologia informatica*, in *Dir. dell'internet,* 2008, p. 228 ss.; ID., *L'inchiesta penale tra echi del passato e risvolti della modernità*, in AA.VV*., Inchiesta penale e pre-giudizio. Una relazione interdisciplinare,* a cura di P. Marchetti, ESI, 2007, p. 29 s.; L. LUPARIA–G. ZICCARDI, *Investigazione penale e tecnologia informatica*. *L'accertamento del reato tra progresso scientifico e garanzie fondamentali,* Giuffrè, 2007, p. 5 ss.; F. MARCELLI, *Internet fra canale di partecipazione politica e strumenti di controllo. Profili di diritto internazionale*, in AA. VV., *La rete internet come spazio di partecipazione politica*. Una prospettiva giuridica, a cura di F. Marcelli–M. Marsocci–M. Pietrangelo, Editoriale Scientifica, 2015, p. 34 ss.; G. MAROTTA, *Innovazioni tecnologiche e diritto al rispetto del domicilio nella Convenzione europea*, in *Riv. dir. internaz*., 2005, f. IV, p. 1044 ss.; L. NANNIPIERI, *La dimensione costituzionale del* digital divice. *In particolare gli ostacoli cognitivi alla proiezione dell'individuo nello spazio virtuale*, in AA. VV., *Internet e Costituzione*, a cura di M. Nisticò–P. Passaglia, Giappichelli, 2014, p. 189; B. SANDYWELL, On *the globalisations of crime: the Internet and new criminality,* in AA. VV., *Handbook of Internet Crime,* a cura di Y. Jewkes–M. Yar, Willan, 2010, p. 38 ss. Più di recente, R. ORLANDI*, La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. proc. pen.,* 2014, f. 3, p. 1151 ss. Da ultimo, C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* cit., p. 1210 ss.

[160] La legge 23 novembre 1993, n. 547, recante *"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"*, in *Gazz. Uff.,* 30 dicembre 1993, n. 305, oltre ad innovare diversi articoli del c.p. (artt. 392; 420; 616; 621; 623 *bis* c.p.) e del c.p.p., ha definito, attraverso l'introduzione dell'art. 491 *bis* c.p., il concetto di «documento informatico» come «[…] qualunque supporto informatico concernente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli». Il legislatore, peraltro,

privata, quella familiare nonché la corrispondenza di un individuo, qualunque intrusione abusiva determina la contemporanea violazione di tutti i corrispondenti diritti protetti sia a livello costituzionale (artt. 14 e 15 Cost.) che convenzionale (art. 8 CEDU)[161].

In questo contesto, rileva nell'immediatezza lo sviluppo naturale del concetto di domicilio fisico, la cui tutela deve necessariamente estendersi anche ai luoghi digitali[162].

---

nell'assoluto convincimento che i reati informatici non fossero altro che nuove forme di aggressione ai beni giuridici già oggetto di tutela nelle diverse parti del codice penale, ha optato per la tecnica dell'"integrazione evolutiva", affiancando le nuove previsioni a quelle fattispecie di reato che ad esse apparissero più vicine. Per quanto concerne i sistemi informatici, il legislatore ha, dunque, ritenuto che essi costituissero «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dell'art. 14 Cost. e penalmente tutelata dagli artt. 614 e 615 c.p.». Così Relazione al disegno di legge n. 2273, poi tradottosi nella suddetta legge. Nel capo III, dedicato ai delitti contro la libertà individuale, del Titolo XII, intitolato «Dei delitti contro la persona», del Libro II c.p., sono stati introdotti gli artt. 615 *ter* («Accesso abusivo ad un sistema informatico o telematico», fattispecie intesa come la «moderna forma di aggressione all'inviolabilità del domicilio». Così G. PICA, *Diritto penale delle tecnologie informatiche*, Utet, 1999, p. 61. Secondo altra parte di dottrina la norma «rafforzerebbe la tutela della segretezza dei dati e dei programmi contenuti in un elaboratore». Cfr. F. MANTOVANI, *Diritto penale. Parte speciale. Delitti contro la persona*, Cedam, 2005, p. 502; F. PAZIENZA, *In tema di criminalità informatica: l'art. 4 della legge 23–12–1993, n. 547*, in *Riv. it. dir. pen. proc.*, 1995, p. 752); art. 615 *quater* («Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici»); art. 615 *quinquies* («Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico», in cui si intravede una tutela del patrimonio informatico, già protetto dall'art. 635 *bis* c.p.). Per approfondimenti sul tema, AA. VV., *Reati contro la persona, vol. 1. Reati contro la vita, l'incolumità individuale e l'onore*, a cura di A. Manna, Giappichelli, 2007, p. 823 ss.; C. PECORELLA*, Il diritto penale dell'informatica*, Cedam, 2006, p. 4338 ss.; L. PICOTTI, voce *Reati informatici*, in *Enc. giur.,* VIII, Treccani, 2000, p. 1 ss.; G. PICA, voce *Reati informatici o telematici*, in *Dig. pen.,* IV, Utet, 2000, p. 521 ss. Successivamente, i *computer crimes* sono stati integrati dalla l. Legge 18 marzo 2008, G.U. n. 80 del 4 aprile 2008, recante *"Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno"*. Numerose sono state le modifica apportate dalla predetta legge al c.p. e al c.p.p.: in particolare è stato modificato l'art. 491 *bis* c.p. (attraverso la soppressione del suo secondo periodo che forniva una definizione pressoché compiuta di documento informatico); nonché l'art. 615 *quinquies* (rubricato, secondo la nuova formulazione, «Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico); sono stati, inoltre, inseriti svariati articoli al fine di apprestare una più adeguata tutela alle svariate ed innumerevoli fattispecie delittuose (*ex plurimis* artt. 635 *ter, quater, quiquies*; nonché l'art. 24 *bis* del d.lgs. 231/2001, in tema di «Delitti informatici e trattamento illecito dei dati»). Cfr. L. LUPARIA, *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul* cybercrime, 2009, p. 72 ss.; C. MAIOLI–E. SANGUEDOLCE, *I "nuovi" mezzi di ricerca della prova fra informatica forense e l. 48/2008*, 3 maggio 2012, in *www.altalex.com*; F.R. FULVI, *La Convenzione* Cybercrime *e l'unificazione del diritto penale dell'informatica*, in *Dir. pen. proc.*, 2009, f. 5, p. 639 s.

[161] In tema già P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, 1997; M. MANTOVANI, *Brevi note a proposito della nuova legge sulla criminalità informatica,* in *Crit. dir.*, 1994, 17 ss.; M. MUCCIARELLI, sub *art. 4 l. 23/12/1993, n. 547,* in *Legislaz. pen.*, 1996, p. 98 ss.; M. NUNZIATA, *La prima applicazione giurisprudenziale del delitto di «accesso abusivo ad un sistema informatico»* ex *articolo 615* ter *c.p.,* in *Giur. mer.,* 1998, p. 711 ss.

[162] Come sostenuto, «[…] la nozione processuale penale di luogo si ricollega all'idea di uno spazio fisico circoscritto. Si tratta di un concetto idoneo a ricomprendere anche qualunque dispositivo informatico, considerato che quest'ultimo corrisponde ad un quid materiale che occupa uno spazio definito in grado di contenere dati. […] I dispositivi informativi possono senz'altro configurarsi alla stregua di luoghi in cui svolgere indagini […]» Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 57. Nello stesso senso, A. PAPA, *Espressione e diffusione del pensiero in internet. Tutela dei diritti e progresso tecnologico*, Giappichelli, 2009, p. 37 ss.

Come rilevato, il c.d. domicilio informatico[163] «non è solo il luogo ove il soggetto avente diritto può esplicare liberamente qualsiasi attività lecita, ma è un'area la cui tutela si estende anche nello *ius excludendi alios*»[164], per cui si ritengono applicabili «tutte le garanzie previste al "domicilio tradizionale"»[165].

Seguendo una simile impostazione, l'interesse all'integrità e alla riservatezza del domicilio informatico rappresenta una «forma di espressione del "tradizionale" diritto di manifestazione della personalità»[166].

Una simile scelta appare ai più semplicistica e poco aderente alle esigenze della modernità[167]. Pur riconoscendo al domicilio informatico la tutela di cui all'art. 14 Cost., la garanzia così come congenata risulta ancora «imperfetta»[168]: in relazione a questo peculiare luogo, infatti, si delinea

---

[163] Il riferimento al «domicilio informatico» si rinviene nella giurisprudenza di legittimità più recente. Così Cass., sez. un., 7 febbraio 2012, n. 4694, in *www.neldiritto.it*. Per commenti, si rinvia a R. FLOR, *Verso una rivalutazione dell'art. 615* ter *c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen. cont.*, 2012, f. 2, p. 126 ss. Nello stesso senso, Cass., sez. un., 24 aprile 2015, n. 17325, in *Proc. pen. giust*., 2015. Sul tema, R. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015, f. 12, p. 1296 ss., cui si rinvia per ulteriori riferimenti bibliografici e giurisprudenziali.

[164] Cass., sez. V, 26 ottobre 2012, n. 42021, in *Dir. e giust*., 29 ottobre 2012. Più di recente, in ordine alla configurabilità della casella di posta elettronica all'interno della più ampia nozione di domicilio informatico, Cass., sez. V, 31 marzo 2016, n. 13057, in *Proc. pen. giust*., 2016. Come anche chiarito, «il *personal computer* non può essere più considerato un semplice strumento di elaborazione e conservazione di documenti in formato elettronico, ma rappresenta un indispensabile mezzo di catalogazione, applicazione e ricerca attraverso il quale l'individuo esprime le sue capacità professionali, culturali e, più in generale, le sue facoltà intellettive». Così L. CUOMO, *La tutela penale del domicilio informatico*, in *Cass. pen*., 2000, f. 11, p. 2998. Sul concetto di domicilio informatico, R. FLOR, *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di "domicilio informatico" e lo* jus excludendi alios, in *Dir. pen. proc*., 2005, f. 1, p. 81 ss.; ID., *Verso una rivalutazione dell'art. 615* ter *c.p.?,* cit., p. 126 ss.; G. MAROTTA*, Innovazioni tecnologiche e diritto al rispetto del domicilio nella Convenzione europea*, cit., p. 1047 ss.; C. PECORELLA, *L'accesso abusivo a sistemi informatici o telematici,* in AA. VV., *Il libro dell'anno 2013,* diretto da R. Chiaberge, Treccani, 2013, p. 49 ss.; L. PICOTTI, *Spunti di riflessione per il penalista della sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, cit., p. 5 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 57 ss.

[165] Cfr. Cass., sez. VI, 4 ottobre 1999, n. 3065, in *Foro it.*, 2000, con nota di A. FANELLI; in *Dir. informazione e informatica*, 2001, p. 492, con nota di G. CORRIAS LUCENTE; in *Cass. pen*., 2000, f. 12, p. 2990, con note di S. ATERNO e di L. CUOMO, in cui gli Autori si soffermano sullo *ius excludendi alios* che qualifica la tutela apprestata dall'art. 615 *bis* c.p., finalizzata ad assicurare la protezione del domicilio informatico quale «spazio ideale di pertinenza della persona». Si veda anche Cass., sez. V, 30 settembre 2008, n. 1727, in *C.E.D. Cass.,* n. 242938, dove si ravvisa il bene tutelato del domicilio informatico sotto il profilo dello *ius excludendi alios*. Per la giurisprudenza di merito, App. Bologna, 30 gennaio 2008, in *Corriere del merito*, 2008, f. 10, p. 1066, con nota di F. D'ARCANGELO; in *Merito*, 2008, fac. 11, p. 57, con nota di A. SORGATO.

[166] L'espressione appartiene a R. FLOR, voce Riserva*tezza informatica*, cit.

[167] In relazione alla peculiarità del bene tutelato dalle norme del codice penale, in dottrina si è spostato l'angolo prospettico dal domicilio alla riservatezza individuando un diritto distinto sia dal domicilio che dalla riservatezza *tout court* e che è stato efficacemente denominato diritto alla "riservatezza informatica". Cfr. L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei* social network. *Aspetti penali*, in *Giur. merito*, 2012, f. 11, p. 2532 ss.; ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in AA. VV., *Il diritto penale dell'informatica all'epoca di internet*, a cura di L. Picotti, Cedam, 2004, p. 87 ss.; R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *Dir. pen. cont.,* 20 settembre 2012.

[168] S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 69.

una plurima necessità di protezione che «finisce per trascenderne i confini fino a confluire nella sfera di tutela di un diritto nuovo […] non certo statico, ma estremamente dinamico»[169].

Ci si trova, in sostanza, dinanzi a un'esigenza di protezione dotata di caratteristiche peculiari: il suo oggetto è l'esclusività dell'accesso ad uno o più spazi informatici, indipendentemente dalla natura dei dati e delle informazioni in essi ospitati, nonché dal livello di indisponibilità di detti elementi rispetto ad illegittime interferenze da parte di terzi[170].

Le guarentigie sin qui considerate, nell'espandersi in direzioni che non potevano essere previste al momento della formulazione del disposto costituzionale, finiscono per convergere in un punto di incontro: un "diritto alla riservatezza informatica", ossia una sorta di diritto all'esclusività dell'accesso a uno o diversi "spazi informatici", da difendere a priori, a prescindere dai loro contenuti[171].Viene, in tal modo, consacrata la genesi di un nuovo bene giuridico tutelabile, definito «diritto all'intangibilità della vita digitale»[172], che a differenza della garanzia della segretezza ed integrità dei sistemi informatici sperimentata dalla Corte costituzionale tedesca[173], non focalizza la propria sfera di protezione sullo strumento informatico in sé considerato ma si concentra sull'individuo, presidiando il suo nuovo «modo di essere nel mondo»[174], la sua

---

[169] Si esprime cosi S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 69. Nello stesso senso anche R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Riv. it. dir. proc. pen*., 2018, f. 2, p. 543, per cui «[S]si pretende di ricavare questo diritto dall'art. 14 Cost. ma […] la nozione di domicilio, nella quale si riflette la proiezione spaziale della persona, è qui solo lo spunto analogico per la costruzione di una nuova, inedita categoria concettuale che ha nell'art. 2 Cost. la sua scaturigine giuridica». In senso conforme, M. MONTAGNA, *Libertà domiciliare*, in AA. VV., *Diritti della persona e nuove sfide del processo penale,* cit., p. 145 s.

[170] In questo senso L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale*, cit., p. 295.

[171] Così R. ORLANDI, *La riforma del processo penale,* cit., p. 1151 ss.

[172] Così denominato da S. SIGNORATO, *Le indagini digitali*, cit., p. 69. Ma già ID., *Le indagini penali informatiche, vol. I, Lessico, tutela dei diritti fondamentali. Questioni generali*, Giappichelli, 2017, p. 71. La necessità di garantire una protezione al nuovo diritto si ritiene poter derivare dalla Risoluzione del Consiglio dei diritti dell'uomo sul diritto alla *privacy* nell'era digitale, doc. A/HRC/28/L.27, 24 marzo 2015.

[173] É la giurisprudenza costituzionale tedesca a consacrare espressamente il diritto all' "*Integrität und Vertraulichkeit informationstechnischer Systeme*". Sul tema, BVerfG, 27 febbraio 2008, 370/2007–595/2007, in *BverfGE* 120, p. 274 ss. Sul punto, R. FLOR, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del Bundesverfassungsgericht e della Curtea Constituţională su investigazioni ad alto contenuto tecnologico e data retention*, in AA. VV., *Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, a cura di L. Picotti–F. Ruggieri, Giappichelli, 2011, p. 32 ss.; ID., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. Online Durchsuchung*, in *Riv. trim. dir. pen. econ.,* 2009, f. 1, p. 695 ss. Inoltre, la Corte costituzionale tedesca ha dichiarato incostituzionale il § 5, comma 2, n. 11, del *Gesetz über den Verfassungsschutz in Nordrhein–Westfalen* – VSG – come modificato il 20 dicembre 2006, in materia di raccolta e trattamento dei dati degli utenti in/da sistemi informatici ed attraverso la rete e, in specie, lo strumento investigativo dell'accesso segreto a sistemi informatici da parte di un'autorità statale di *intelligence*, da utilizzare nel rispetto di alcuni (inadeguati) parametri legali (cd. *Online Durchsuchung*). Sul punto si rinvia a F. IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. pen. cont.*, 22 luglio 2014, p. 329 ss.; S. MARCOLINI, *Le cosiddette perquisizioni online* (*o perquisizioni elettroniche*), in *Cass. pen.*, 2010, f. 11, p. 2855 ss.; F. CAJANI, *Odissea del captatore informatico*, cit., p. 4143 ss. Si veda, altresì BVerfG, 20 aprile 2016, BVR 966/09, 1 BVR 1140/09, in *Dir. pen. cont.,* 8 maggio 2016.

[174] Così S. RODOTÁ, *Il mondo nella rete,* cit., p. 102. Nello stesso senso L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali: verso nuovi orizzonti di tutela nell'accertamento penale,* cit., p. 291.

soggettività in rapporto a qualunque dato o attività svolta nell'ambito di un sistema informatico e della rete.

Un diritto alla «libertà informatica»[175], la cui tutela potrebbe essere ricompresa nell'alveo dell'art. 2 Cost.[176], ovvero ricavata da una norma sovra-legale (CEDU) interposta alla Costituzione[177].

Riconoscere l'esistenza di moderne prerogative individuali non rappresenta una velleità dogmatica, traducendosi, sul piano processuale, nella sottoposizione dell'uso investigativo dei captatori informatici alla nota procedura che le costituzioni moderne esigono per la compressione di diritti considerati inviolabili: vale a dire, riserva di legge e autorizzazione giudiziale nel rispetto del principio di proporzionalità.

Il rischio, altrimenti, è quello di lasciare alla polizia ampi spazi di iniziativa informale e atipica, con l'uso
di strumenti invasivi della sfera intima della persona. Solo attraverso il riconoscimento delle nuove prerogative individuali, le altre attività esperibili mediante captatore informatico andrebbero considerate illegittime fino a che non saranno regolate da una norma volta ad attuare le accennate garanzie procedurali imposte dalla costituzione per la limitazione dei diritti inviolabili.

Per onestà intellettuale, tuttavia, bisogna ammettere che il riconoscimento solo empirico dei nuovi diritti non rende più sereno lo studioso. Si sa che un precetto, per essere concreto, deve trasformarsi in "diritto vivente", trovando un effettivo riscontro nella prassi giudiziaria. Ma attualmente sembra ancora utopica la concezione di offrire una protezione totalizzante alle prerogative di un individuo che estrinseca il suo *ego* nella rete, preferendo il legislatore prevedere una tutela "settorializzata" alle prerogative soggettive, ossia una protezione che risulta ancora indissolubilmente legata alle *species* di violazioni perpetrate.

6. SICUREZZA *VS* LIBERTÀ: ALLA RICERCA DI UN DIFFICILE EQUILIBRIO

In tema di contrasto ai fenomeni criminali di particolare rilevanza sociale si registrano, da sempre, forti tensioni tra esigenze di accertamento dei reati e tutela dei diritti fondamentali.

La disciplina delle intercettazioni mediante captatore informatico ne rappresenta una prova lampante: dall'analisi dei profili di compatibilità dell'istituto *de qua* con l'ordinamento costituito, infatti, sembra che la normativa, così come congegnata, dia luogo a plurimi sospetti di incostituzionalità, offrendo al processo elementi «raccolti con modalità non disciplinate dal codice di rito e lesive dei diritti dell'individuo», tutelati dalla Carta Costituzionale[178].

Lo studioso, tuttavia, è tenuto a fare i conti con la realtà contingente e deve prendere atto che, pur determinando un'ingerenza al godimento delle prerogative individuali riconosciute nella

---

[175] R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici,* cit., p. 543.

[176] Nella dottrina italiana, la tesi dell'art. 2 cost. come "fattispecie aperta" sul cui terreno possono germogliare "nuovi diritti" è convintamente sostenuta da A. BARBERA, sub *art. 2*, in *Commentario della Costituzione*, a cura di G. Branca, Zanichelli, 1976, p. 80 ss.

[177] Come precisa R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 544, «[I]nadeguato sarebbe, a questo riguardo, il richiamo all'art. 8 CEDU posto a tutela della sfera individuale nei rapporti familiari e interpersonali. Esso copre certamente il diritto alla privacy, non quello all'uso libero e riservato dei sistemi informatici. Lo stesso discorso vale per l'art. 8 della Carta dei diritti fondamentali UE, posto a protezione dei dati di carattere personale».

[178] Così si esprime V. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, cit., p. 341. Definizione poi ripresa da C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 151.

Carta fondamentale, i risultati ottenibili attraverso l'espletamento delle indagini proattive sono assai efficaci nella repressione delle più gravi fattispecie delittuose, per cui non è prospettabile che il sistema penale ne rimanga del tutto privo[179].

D'altra parte, il ricorso alle moderne tecniche di captazione risponde all'esigenza di contenere i fenomeni criminali, tutelando il più generale bisogno di sicurezza[180] individuale e collettiva[181], quale bene costituzionale «imprescindibilmente legato alla vita, all'incolumità fisica, al benessere dell'uomo e alla qualità della sua esistenza, nonché alla dignità della persona»[182].

Rebus sic stantibus, sembrerebbe che l'enigma possa trovare soluzione attraverso il riconoscimento del valore che deve essere considerato "primario", potendosi in tal modo legittimare la soccombenza del più debole rispetto al più forte[183].

In questo gioco di forze, c'è chi ritiene che l'esigenza di sicurezza rappresenti il bene giuridico fondamentale, la cui protezione legittima «un netto restringimento o […] il completo annullamento delle garanzie dei soggetti coinvolti»[184] e chi, per converso, ritiene imprescindibile

---

[179] «Il rito penale deve certo ispirarsi alle innovazioni tecnologiche: la criminalità si evolve, si attrezza, diventa sempre più subdola e pericolosa; a tale progresso deve adeguarsi il processo, pena la trasformazione in un'arma spuntata, inidonea a raggiungere lo scopo». Così C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* cit., p. 1210.

[180] La dottrina, in particolare quella costituzionalistica, si è lungamente interrogata sulla definizione di sicurezza e sul suo fondamento costituzionale. Sul tema, diffusamente, M. DOGLIANI, *Il volto costituzionale della sicurezza*, in AA. VV., *I diversi volti della sicurezza*, a cura di G. Cocco, Giuffrè, 2012, p. 1 ss.; S.W. BRENNER, *Cybercrime, cyberterrorism and cyberwarfare*, in *Revue internationale de droit penal*, 2007, p. 453 ss; C. SARZANA DI SANT'IPPOLITO, *Sicurezza informatica e lotta alla* cybercriminalità: *confusione di competenze e sovrapposizione di iniziative amministrative e legislative,* in *Diritto dell'Internet*, 2005, f. 5, p. 437 ss.

[181] Con riguardo ai fondamenti costituzionali della sicurezza, le due posizioni prevalenti sono quelle che tendono a individuare, da un lato, la sicurezza come interesse collettivo riconosciuto, e, dall'altro, la sicurezza come vero e proprio diritto fondamentale proprio di ciascun individuo. Sul primo aspetto, A. PACE, *Libertà e sicurezza. Cinquant'anni dopo,* in AA. VV., *Costituzioni e sicurezza dello Stato,* a cura di A. Torre, Maggioli, 2014, p. 551, secondo cui «sicurezza pubblica e ordine pubblico costituiscono non già concetti diversi tra loro ma i due lati della stessa medaglia, il primo soggettivo, il secondo oggettivo». Viceversa, tra coloro che ritengono che la sicurezza rappresenti un'esigenza non del singolo ma della collettività, M. DOGLIANI, *Il volto costituzionale della sicurezza*, cit., p. 1 ss.; P. RIDOLA, *Libertà e diritti nello sviluppo del costituzionalismo*, in AA. VV., *I diritti costituzionali,* a cura di R. Nania–P. Ridola, cit., p. 4

[182] Così G. CERRINA FERONI–G. MORBIDELLI, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, n. 1, 2018. Nello stesso senso, T.E. FROSINI, *Il diritto costituzionale alla sicurezza*, in *Forum* online *di Quaderni costituzionali*.

[183] La dottrina, in sostanza, si domanda quale possa mai essere nella società moderna il confine tra legittimo bisogno di sicurezza dei cittadini e il rispetto delle prerogative individuali, «paventando derive verso quella che è stata definita la "società della sorveglianza"». Così A. GAITO–S. FURFARO, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza*, cit., p. 364, i quali sottolineano come «si va, pian piano, ma decisamente, verso il "paradosso della libertà"».

[184] Così A.M. DERSHOWITZ, *Why Terrorism Works. Understanding the Threat, Responding to the Challenge*, Yale University Press, 2002. Nello stesso senso le teorie di Niklas Luhmann e di Günther Jakobs. Il primo muove dal c.d. *ticking time bombe* scenario, ossia dall'ipotesi in cui la polizia riesca ad arrestare il capo di una pericolosa organizzazione criminale in grado di svelare notizie fondamentali per prevenire un imminente attacco terroristico. Al riguardo, il filosofo si chiede se fosse possibile torturare il capo dell'organizzazione terroristica pur di ottenere le informazioni neccessarie, oppure, per converso, se valesse, anche in tale ipotesi estrema, l'obbligo di tutela i diritti individuali fondamentali. Luhmann finisce per ritenere che in un simile contesto la tortura potrebbe essere ammessa perché lo Stato deve in primis soddisfare le esigenze di protezione della collettività. Cfr. N. LUHMANN, *Sistemi sociali. Fondamenti di una teoria generale*, Il Mulino, 2001, p. 12 ss. Si tratta di una teoria simile a quella sostenuta più di recente da Jakobs, il quale distingue tra *Bürgerstrafrecht* (diritto penale del cittadino) da un *Feindstrafrecht* (diritto penale del nemico). Il

considerare la sussistenza di un nucleo di diritti inviolabili che, indipendentemente dal contesto, non possono subire compressioni[185].

A ben guardare, nessuna delle due prerogative sembra potersi atteggiare come preminente sull'altra: libertà e sicurezza, non rappresentano valori contrastanti ma due facce della stessa medaglia, parimenti meritevoli di tutela per l'ordinamento costituito[186].

Non parendo, allora, possibile operare in ragione di un criterio "gerarchico", il "moderno" giurista si trova a dover operare un complesso bilanciamento tra le due forze centrifughe; bilanciamento che «è sempre ricompreso tra diritti fondamentali. Anche quando vengono chiamati in causa interessi fondamentali della collettività (sicurezza, salute, etc.) è necessario, sia per il legislatore che per gli interpreti, scomporre idealmente l'interesse generale invocato, per vedere se la lesione ipotizzata, che giustifica la limitazione, colpisca uno o più diritti fondamentali compresi nell'area del principio invocato in opposizione»[187].

Allora l'obiettivo del giurista è quello di ricerca il delicato equilibrio tra l'esigenza di repressione dei reati, facilitata dal frequente utilizzo di nuovi strumenti di indagine[188], e la

primo andrebbe riferito ai soggetti che, pur commettendo reati, non constestano i fondamenti su cui si regge lo Stato; il secondo, invece, dovrebbe essere applicato a coloro che compiono azioni criminose proprio per sovvertire quei fondamenti, in quanto tali soggetti devono essere considerati come "non persone". Così G. JAKOBS, *Sistema dell'imputazione penale,* Editoriale Scientifica, 2017, p. 5 ss. V., altresì, G. JAKOBS, *I terroristi non hanno diritti*, in AA. VV., *Contrasto al terrorismo interno ed internazionale*, a cura di R.E. Kostoris–R. Orlandi, Giappichelli, 2006, p. 3 ss. Parla di "*Tätertipe"*, ossia della necessità di teorizzare la "tortura legale", già, A. CALVI, T*ipo criminologico e tipo normativo d'autore,* Padova, 1967, p. 50 ss. La tesi dell'esistenza di un "diritto penale del nemico" è ampiamente criticata da R.E. KOSTORIS, *Processo penale, delitto politico e "diritto penale del nemico"*, in *Riv. it. dir. proc. pen*., 2007, f. 1, p. 7 ss., secondo cui «la distinzione tra "diritto penale del cittadino" e "diritto penale del nemico" si compendia in una sorta di paradosso, dato che essa riveste delle forme di del diritto (sia pure del nemico) qualcosa che in realtà nega il diritto stesso o, meglio, le regole minime del diritto di uno Stato di diritto modernamente inteso». Secondo G. CERRINA FERONI– G. MORBIDELLI, *La sicurezza: un valore superprimario*, cit., la sicurezza non è solo un diritto costituzionale, ma «un valore superprimario», che, in quanto tale, non si presta al bilanciamento secondo i canoni tradizionali.

[185] In questo senso R. ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali*, in AA. VV., *La giustizia penale preventiva. Ricordando Giovanni Conso*, Giuffrè, 2016, p. 17 ss., per cui «[L]la Costituzione esclude il perseguimento dello scopo della sicurezza assoluta a prezzo dell'annullamento della libertà» (*Bundersverfassungsgericht*, 1 BvR 518/02).

[186] In questo senso A. MARANDOLA, *Sicurezza e diritti fondamentali: aspetti processuali,* in *Proc. pen. giust.,* 2019, f. 11, p. 1553 ss. Secondo P. ZANON, Un diritto fondamentale alla *sicurezza?, ivi*, p. 1555, anche la sicurezza rientra a pieno titolo tra i diritti personali e primari, perfettamente conformi allo Stato di diritto.

[187] Si esprime così G. SILVESTRI, *L'individuazione dei diritti della persona*, cit., p. 9

[188] In tema di fecondità dell'evoluzione delle cognizioni scientifiche e tecnologiche, cfr. G. CANZIO, *Prova scientifica, ragionamento probatorio e libero convincimento del giudice nel processo penale*, in *Dir. pen. proc*., 2003, p. 1193 s.; G. DI CHIARA, *Il canto delle sirene. Processo penale e modernità scientifico–tecnologica: prova dichiarativa e diagnostica della criminalità*, in *Criminalia*, 2007, f. 1, p. 21 s.; O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico–tecnici nuovi o controversi e di elevata specializzazione*, Giuffrè, 2005, p. 11 s.; ID., *In tema di nuova prova scientifica*, in *Dir. pen. proc*., 2001, f. 10, p. 1061; F. IOVENE, *Le c.d. perquisizioni* online *tra nuovi diritti fondamentali ed esigenze di di accertamento penale,* cit., p. 346; S. LORUSSO, *La prova scientifica*, in AA. VV., *La prova penale*, cit., p. 296 s.; P. TONINI, *Progresso tecnologico, prova scientifica e contraddittorio*, in AA. VV., *La prova scientifica nel processo penale*, a cura di L. De Cataldo Neuburger, Cedam, 2007, p. 57 s. Da ultimo, F. NICOLICCHIA, *Il principio di proporzionalità nell'era del controllo tecnologico e le sue implicazioni processuali rispetto ai nuovi mezzi di ricerca della prova*, in *Dir. pen. cont*., 8 gennaio 2018.

protezione dei diritti individuali inviolabili[189], al fine di scongiurare il rischio di un'«eccedenza dell'esigenza di giustizia rispetto alle possibilità di realizzazione umane»[190].

[189] La necessità della misura, nell'ambito di una società democratica, che garantisca la tutela dei diritti dei singoli e della collettività, «impone il giusto bilanciamento tra le esigenze di tutela degli interessi generali e la protezione dei diritti individuali». Così Corte EDU, Grande camera, 7 luglio 1989, *Soering c. Regno Unito*, n. 14038/88, in *Riv. it. dir. proc. pen.,* 1990, f. 1, p. 334 ss. Sulle problematiche relative al bilanciamento fra diritti fondamentali e contrasto al terrorismo, si sono espressi diversi autori, fra cui B. Ackerman, esponente della corrente di pensiero che sostiene la necessità di introdurre in costituzione una clausola per gli stati di emergenza terroristica che permetta di adottare misure operative efficaci e che, allo stesso tempo, stabilisca con fermezza un limite alla loro durata. In altre parole, una clausola costituzionale d'emergenza che autorizzi deroghe alla garanzia ordinaria dei diritti senza arrivare mai, però, all'estremo della sospensione dell'ordinamento democratico. cfr. B. ACKERMAN, *La Costituzione d'emergenza*, Maltemi, 2005. Altri autori, invece, sostengono la possibilità di applicare in via analogica l'art. 78 della nostra Costituzione all'emergenza terroristica. A tal proposito, si veda P. CARNEVALE, *Emergenza bellica e sospensione dei diritti costituzionalmente garantiti. Qualche prima considerazione anche alla luce dell'attualità,* in *Giur. Cost.,* 2002, f. ?, p. 4526 ss. Volendo richiamare un'autorevole dottrina, espressasi sul tipo di ragionamento che presiede all'applicazione dei diritti fondamentali ad opera della giurisdizione di costituzionalità, potrebbe delinearsi la distinzione prospettata fra regole e principi, in tal caso «la forma di applicazione delle regole, è la sussunzione. La forma di applicazione dei principi è il bilanciamento». Aderendo a questo schema il principio della proporzionalità consta di tre regole: l'idoneità (della misura a raggiungere lo scopo), l'indispensabilità della stessa e la giustificabilità del sacrificio imposto rispetto alla gravità del reato (proporzionalità in senso stretto). Tali regole possono essere definite tali in quanto «non sono bilanciate contro qualcosa d'altro. Esse non hanno una volta la prevalenza e un'altra non l'hanno più. Piuttosto s'indaga se i sotto–principi siano realizzati o no, e se la non realizzazione abbia come conseguenza l'antigiuridicità» Dunque, se i sotto principi vengono realizzati, permettono una ponderazione, fondata sulla proporzionalità, tra l'inviolabilità della libertà individuale e la tutela di interesse collettivo alla repressione dei reati, e il criterio discretivo alla luce del quale è consentita tale ponderazione è la ragionevolezza. Cfr. R. ALEXY, *Teoria dei diritti fondamentali,* Il Mulino, 2012, p. 107. Stando alla definizione proposta da Alexy «le regole sono norme che possono essere sempre realizzate o non realizzate», sicché, «se una regola è valida, allora è obbligatorio fare esattamente ciò che essa richiede». Sono al contrario principi, secondo Alexy, le norme che consistono in «mandati di ottimizzazione», cioè in norme che dispongono che «qualcosa sia realizzato nella maggior misura possibile sulla base delle circostanze di fatto e di diritto».

[190] Si esprime così M. CARTABIA, *Edipo re*, in AA VV., *Giustizia e mito*, a cura di M. Cartabia –L. Violante, Il Mulino, 2018, p. 50.

A tal fine, il "faro" che guida le scelte di politica criminale deve essere rappresentato dal principio di proporzione[191] – o, meglio, della ragionevolezza[192] – della misura rispetto allo scopo perseguito, nel senso che qualunque restrizione dei diritti fondamentali non può risultare eccedente rispetto alla gravità dei motivi che la giustificano, nel completo rispetto del principio di "stretta necessità"[193].

La proporzionalità, pur non essendo sinonimo di "giustizia" od "equità", può essere considerato il corollario dell'inviolabilità delle prerogative individuali che, inevitabilmente sono

[191]Come precisato, «[L]la proporzionalità evoca […] una correlazione del mezzo rispetto al fine, nel senso che tra strumento normativo regolatore e realizzazione del fine che con esso si intende perseguire, l'opera di "bilanciamento" deve condurre ad un equilibrato componimento dei sacrifici». Così A. MACCHIA, *Il controllo costituzionale di proporzionalità e ragionevolezza*, in *Cass. pen.,* 2020, f. 1, p. 19 ss. Il tema è assai vasto nel panorama dottrinale e giurisprudenzuale. Sul bilanciamento di interessi contrapposti, senza pretese di completezza, più di recente, M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, Roma, Palazzo della Consulta 24-26 ottobre 2013, Conferenza trilaterale delle Corti costituzionali italiana, portoghese, spagnola; E. COTTU, *Giudizio di ragionevolezza e vaglio d proporzionalità della pena: verso il superamento del modello triadico?,* in *Dir. pen. proc*., 2017, f. 3, p. 473 ss.; V. MANES- V. NAPOLEONI, *La legge penale illegittima*, Giappichelli, 2019, p. 362 s.; MANES, *Principio di proporzionalità. Scelte del legislatore e sindacato di legittimità,* in *Libro dell'anno del diritto*, Treccani, 2013, p. 104; A. MERLO, *Considerazioni sul principio di proporzionalità nella giurisprudenza costituzionale in materia penale,* in *Riv. it. dir. e proc. pen*., 2016, p. 1427; A. MORRONE, voce *Bilanciamento (giustizia costituzionale),* in *Enc. dir.,* Annali, vol. II, t. II, Giuffrè, 2008, p. 187 s.; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *Riv. it. dir. proc. pen*., 2020, f. 1, p. 3 ss.; ID., *Compressione dei diritti di libertà e principio di proporzionalità*, in AA. VV., *Diritti della persona e nuove sfide del processo penale,* cit., p. 55 ss.; G. SCACCIA, *Proporzionalità e bilanciamento dei diritti nella giurisprudenza delle Corti europee*, in *Rivista AIC,* 2017, n. 3.

[192] Parte della dottrina costituzionalistica ritiene "più conveniente" ricorrere al criterio di ragionevolezza, in quanto «se la proporzione fosse rigorosamente numerica, si tratterebbe di un criterio più preciso di quello, indeterminato, della ragionevolezza, i cui risultati sono sempre opinabili. Ma non è così. Stabilire se due entità sono tra loro in rapporto di proporzionalità involve una serie di valutazioni e giudizi di valore, che difficilmente consentono di ricavare un risultato certo. Quando un bilanciamento rispetta il criterio di proporzionalità? Risposta: quando il legislatore o l'interprete ritengono che il punto di equilibrio formulato sia giusto, non in via logico–razionale, ma in quanto "ragionevolmente" accettabile, alla luce di opzioni culturali, politiche, sociali etc. La ragione empirica, con tutta la sua carica di "vaghezza", scacciata dalla porta, rientra dalla finestra. Ciò a parte ogni considerazione sulla cosiddetta irragionevolezza "intrinseca" (es. norma autocontraddittoria), che resta fuori del perimetro della proporzionalità. Non si tratta di una mera dissertazione teorica, ma di una sottolineatura della necessità di non illudersi di "imbrigliare" l'elasticità delle valutazioni con formule solo apparentemente quantitative». Così G. SILVESTRI, *L'individuazione dei diritti della persona*, cit., p. ?. Sul punto, v. anche A. MACCHIA, *Il controllo costituzionale di proporzionalità e ragionevolezza*, cit., p. 19 ss., per cui «[L]la ragionevolezza, essendo "figlia" della uguaglianza, tende a spostarsi più sul versante comparativo […], il quale evoca, da vicino, la tematica del giudizio c.d. triadico o diadico». Su tre aspetti della ragionevolezza, in AA.VV., *Il principio di ragionevolezza nella giurisprudenza della corte costituzionale,* Giuffrè, 1994, p. 180 s.; V. MANES, *Attualità e prospettive del giudizio di ragionevolezza in materia penale,* in *Riv. it. dir. e proc. pen*., 2007, f. ?, p. 741.

[193] R. FLOR, *La tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del* Bundesverfassungsgericht e della Curtea Constituţională *su investigazioni ad alto contenuto tecnologico e data retention,* in *Nuove tendenza della giustizia penale di fronte alla criminalità informatica*, a cura di F. Ruggieri–L. Picotti, Giappichelli, 2011, p. 31 ss.

poste in tensione dall'esperimento di attività investigative "segrete", dirette all'apprensione di dati e informazioni per neutralizzare la minaccia[194].

In effetti, il principio *de quo*, lungi dal rimanere confinato al ruolo di mero enunciato normativo astratto, rappresenta assai spesso il più importante momento di verifica in cui si articola il complesso giudizio di legittimità delle disposizioni nazionali limitative delle prerogative individuali[195].

---

[194] Si esprime così M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale,* in *Dir. pen. cont*., n. 3/4, 2014, p. 147 s.

[195] Basti pensare, solo a titolo esemplificativo, alla nota pronuncia della Corte di giustizia che, in applicazione dei principi di legalità e proporzione, ha censurato la normativa europea in materia di acquisizione e conservazione dei dati inerenti al traffico telefonico a scopi di indagine, accertamento e perseguimento di reati. In particolare, la Corte ha osservato anzitutto che i dati da conservare consentono di conoscere l'identità della persona con la quale un utente registrato ha comunicato e con quali mezzi; identificare il momento e il luogo della comunicazione; conoscere la frequenza delle comunicazioni dell'utente con determinate persone inunospecifico periodo. Tali dati, nel complesso, possono fornire informazioni molto precise sulla vita privata delle persone i cui dati sono conservati, come ad esempio le abitudini della vita quotidiana, i luoghi di residenza, i movimenti, le attività svolte, le relazioni sociali e gli ambienti frequentati. In merito a ciò, ha ritenuto che, imponendo la conservazione di tali dati e permettendo alle autorità nazionali competenti di accedere a tali dati, la direttiva interferisce in modo eccessivo con i diritti fondamentali del rispetto della vita privata e della protezione dei dati personali. Inoltre, il fatto che i dati siano conservati e utilizzati senza che l'utente ne sia previamente informato, può ingenerare negli interessati un sentimento di soggezione a una costante sorveglianza. La Corte ritiene che «[…] la conservazione dei dati genetici, pur in astratto giustificata dall'obiettivo di interesse generale di prevenzione dei reati gravi, realizza un'ingerenza non conforme al principio di proporzionalità». CGUE, Grande Sezione, 8 aprile 2014, cit., § 45 ss., annotata da R. FLOR, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. "*data retention*" contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *Dir. pen. cont*., 2014, n. 2, p. 178 ss. Sul tema, L. TRUCCO, Data retention*: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. it.,* 2014, f. 8–9, p. 1850 ss.; F. FABBRINI, *The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 *Harvard Human Rights Journal,* 2015, p. 65 ss.; F. IOVENE, Data retention *tra passato e futuro. Ma quale presente?,* in *Cass. pen*., 2014, f. 5, p. 808 ss.; E. COLOMBO, "Data retention" *e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della direttiva 2006/24/CE*, in *Cass. pen.,* 2014, p. 2705 ss.; M.–P. GRANGER – K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and* Data Protect*ion*, in *Eur. Law Rev*., n. 39, 2014, p. 83 ss.; M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* data retention, in *Dir. dell'Unione eur.,* 2014, f. 4, p. 803 ss. Da ultimo, S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014,* in AA. VV., Cybercrime, cit., p. 1579 ss. Nello stesso senso, anche la recente pronuncia della Corte di Giustizia, chiamata a pronunciarsi sulla portata dell'art. 15 par. 1 della direttiva 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche. In quell'occasione i giudici hanno avuto modo di di chiarire come tale previsione osti ad una normativa nazionale che non limiti l'accesso da parte delle autorità domestiche ai dati conservati dai gestori dei servizi di comunicazione per sole finalità di lotta contro la criminalità grave, non sottoponga detto accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente e non esiga la conservazione dei dati nel territorio dell'Unione. In particolare, Gli Stati membri, secondo la Corte, non possono imporre ai fornitori di servizi di comunicazione elettronica un obbligo generale e indifferenziato di conservazione dei dati di traffico e di ubicazione degli utenti. Una conservazione preventiva di tali dati è ammessa, purché risulti mirata e limitata allo stretto necessario per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista. Inoltre, quanto all'accesso delle autorità nazionali competenti ai dati conservati, la conservazione deve avvenire in base a criteri oggettivi e rispettare determinate condizioni, tra cui un

Più in particolare, lo scrutinio di ragionevolezza, in questi ambiti, impone di verificare che il bilanciamento degli interessi costituzionalmente rilevanti non sia stato realizzato con modalità tali da determinare il sacrificio o la compressione di uno di essi in misura eccessiva e pertanto incompatibile con il dettato costituzionale.

Tale giudizio deve svolgersi «attraverso ponderazioni relative alla proporzionalità dei mezzi prescelti dal legislatore nella sua insindacabile discrezionalità rispetto alle esigenze obiettive da soddisfare o alle finalità che intende perseguire, tenuto conto delle circostanze e delle limitazioni concretamente sussistenti»[196].

Ma non solo.

---

controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente; i dati di cui trattasi devono, infine, essere conservati nel territorio dell'Unione CGUE, Grande Sezione, 21 dicembre 2016, cause C–203/15 e C–698/15, annotata da O. POLLICINO–M. BASSINI, *La Corte di giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico telefonico per finalità di sicurezza e ordine pubblico*, in *Dir. pen. cont.*, 9 gennaio 2017; G. TIBERI, *Il caso* "Tele2 Sverige/Watson": *un'iconica sentenza della Corte di Giustizia nella saga sulla* "data retention", in *Quaderni cost.*, 2017, p. 434 ss. Ma già, CGUE, Grande Sezione, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González,* causa C–131/12, in *Dir. inf.,* 2014, p. 535. Per commenti, G. RESTA–V. ZENO ZENCOVICH, *Il diritto all'oblio su internet dopo la sentenza Google Spain*, RomaTre Press, 2015. Sul punto anche CGUE, 6 ottobre 2015, C–362/14, *Maximillian Schrems c. Data Protection Commissioner.* Circa «l'importanza centrale» del principio di proporzionalità nell'ordinamento giuridico dell'Unione, G. SCACCIA, *Il principio di proporzionalità*, in AA. VV., *L'ordinamento europeo. L'esercizio delle competenze*, a cura di S. Mangiameli, Giuffrè, 2006, p. 225. Anche la Corte EDU segue la medesima impostazione assiologica. Esemplificativo a tale riguardo è quanto stabilito dalla Corte EDU, Grande Camera, 4 dicembre 2008, Marper c. Regno Unito, cit., in relazione alla materia delle banche dati del DNA a scopo investigativo penale. Nel caso in questione, la Corte di Strasburgo ritiene che la normativa del Regno Unito che prevede la conservazione illimitata dei profili genetici dei soggetti indagati violi il diritto al rispetto della vita privata riconosciuto dalla Convenzione Europea dei Diritti dell'Uomo. Ciò in quanto «il carattere generale ed indifferenziato con cui opera il meccanismo di conservazione […] dei profili di DNA di individui sospettati della commissione di determinati reati che però non sono poi condannati […] non garantisce un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco […] Ne segue che [tale] conservazione dei dati personali […] costituisce una ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata; tale ingerenza non può essere considerata come necessaria in una società democratica». Più di recente, i giudici di Strasburgo hanno riconosciuto l'illegittimità dell'ingerenza statale consistente nell'esame del contenuto di un apparecchio informatico effettuato all'insaputa del proprietario ed in assenza di una preventiva autorizzazione giurisdizionale, riscontrando appunto in questo *modus procedendi* una lesione del principio di proporzionalità specie in ragione della considerevole intrusività della misura disposta. Corte EDU, sez. III, 30 maggio 2017, *Trabajo Rueda c. Spagna*, n. 32600/12, §42 ss. Nello stesso senso, anche Corte EDU, sez. V, 27 aprile 2017, *Sommer c. Germania*, n. 73607/13, § 53.

[196] Così Corte Cost., 27 febbraio 2015, n. 23, in *www.cortecostituzionale.it.*

Soprattutto nell'ultimo tempo, il canone di proporzione guida le scelte della giurisprudenza internazionale[197] (e anche interna)[198], tutte le volte in cui ci si trova al cospetto di situazioni "nuove", non compiutamente disciplinate nell'ordinamento di riferimento.

[197] La Germania costituisce un importante punto di riferimento in materia, essendo stato il primo Paese europeo ad autorizzare forme di captazione occulta mediante strumenti di controllo a distanza e, nel contempo, a dubitare sulla liceità degli stessi. *Bundersverfassungsgericht,* 20 aprile 2016, BVR 966/09, 1 BVR 1140/09. Nell'occasione la Corte ha dichiarato l'incostituzionalità di alcune disposizioni della legge federale denominata "*Bundeskriminalamtgesetz*", che disciplina i compiti e l'attività della forza di polizia federale (*Bundeskriminalamt*) e la cooperazione in materia penale tra i Governi statali e quello federale e con i Paesi terzi. Sulla stessa scia della pronuncia del 2008 (BVerfG, 27 febbraio 2008, BVerfGE 120, cit.) il *Bundesverfassungsgericht* riconosce in capo al legislatore il dovere di effettuare un bilanciamento tra la protezione che lo Stato deve accordare ai cittadini e i diritti fondamentali vantati dagli stessi, e tale bilanciamento deve essere condotto nel rispetto del principio di proporzionalità, base al quale «i poteri investigativi che incidono in maniera profonda sulla vita privata vanno limitati dalla legge alla tutela di interessi sufficientemente rilevanti nei casi in cui sia prevedibile un pericolo sufficientemente specifico a detti interessi». Più precisamente, nella sentenza in commento vengono distinte due ipotesi: le disposizioni relative all'uso di mezzi speciali di sorveglianza in luoghi diversi dal domicilio ("*outside of homes"),* come l'osservazione, la registrazione audio–video, l'applicazione di dispositivi di localizzazione o l'uso di informatori della polizia, non rispettano il principio di proporzionalità non limitando i poteri della polizia federale; le disposizioni relative all'uso di tali mezzi nei luoghi domiciliari, rispetterebbero, invece, tale principio, in quanto, da una parte, determinando il monitoraggio dei contatti e delle frequentazioni, non può colpire i terzi estranei, se non in modo meramente indiretto; dall'altra, costituendo un'ingerenza nel nucleo profondo e caratterizzante la vita privata, dopo la realizzazione dell'attività investigativa, salvo i casi di pericolo immediato, i dati raccolti devono essere esaminati da un organismo indipendente, per verificare se contengono informazioni molto private, prima che possano essere utilizzati dalla polizia federale. In dottrina, L. GIORDANO–A. VENEGONI, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Dir. pen. cont.,* 8 maggio 2016; P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*, in *Proc. pen. giust.*, 2016, p. 128 ss.; F. NICOLICCHIA, *I limiti fissati dalla Corte costituzionale tedesca agli strumenti di controllo tecnologico occulto: spunti per una trasposizione nell'ordinamento italiano*, in *Arch. pen*., 2017; W. NOCERINO, *Le Sezioni Unite risolvono l'enigma*, cit., p. 3555 ss.

[198] Nel panorama nazionale si riscontra una sensibile differenza di approccio rispetto a quanto segnalato in relazione al contesto sovrastatale. Per la prima volta nel 2005 la Consulta consacra l'autonomia del criterio in esame allorquando – pronunciandosi sull'illegittimità costituzionale dell'art. 304, comma 6 c.p.p., «nella parte in cui, facendo riferimento all'art. 303, comma 2 c.p.p. ai fini del calcolo della durata massima dei termini di fase di custodia cautelare, non consente di computare i periodi di custodia cautelare sofferti in diversa fase processuale» – sancisce che «[L]le limitazioni della libertà connesse alle vicende processuali devono rispettare il principio di proporzionalità, posto che contrasterebbe con il giusto equilibrio tra le esigenze del processo e la tutela della libertà una disciplina della detenzione cautelare priva di limiti di durata […]. Proporzionalità e ragionevolezza stanno alla base del principio secondo cui, in ossequio al *favor libertatis* che ispira l'art. 13 Cost., deve comunque essere scelta la soluzione che comporta il minor sacrificio della libertà personale». Così Corte cost., 7 luglio 2005, n. 299, in *www.giurcost.org*. Riconosce, seppur implicitamente, la necessità del rispetto del principio di proporzionalità, Corte cost., sent. 24 gennaio 2017, n. 20. La pronuncia della consulta inerisce all'ambito di operatività dell'art. 266 c.p.p., denunciato di incostituzionalità ove restrittivamente interpretato nel senso di non ammettere un potere di controllo occulto della corrispondenza dei detenuti al di là dalle specifiche previsioni dettate dall'art. 18 *ter* dell'ordinamento penitenziario, la consulta smentisce l'ammissibilità dell'interpretazione estensiva proposta dal giudice rimettente, rigettando al contempo la questione di legittimità costituzionale proposta. Viene, infatti, precisato che il bilanciamento operato in concreto dal legislatore tra tutela della riservatezza nelle comunicazioni e repressione degli illeciti penali attraverso la formulazione dell'art. 266 c.p.p., non consentiva di riscontrare «limitazioni irragionevoli o sproporzionate dell'uno o dell'altro» interesse. Per un

In effetti, il principio *de qua* deve rappresentare la "stella polare" che guida e veicola anche le scelte normative, per cui tutte le volte in cui ci si trovi a dover normare un inedito atto idoneo a comprimere i diritti fondamentali, il legislatore non deve essere governato esclusivamente da "libero arbitrio", giacché la disciplina deve soddisfare requisiti assai stringenti: occorre che la misura limitativa sia idonea a raggiungere lo scopo e risulti indispensabile per conseguire quel fine; inoltre, il sacrificio imposto al bene giuridico deve essere giustificato dalla gravità del reato[199].

Alla luce di quanto esposto, possono trarsi delle considerazioni di carattere sistemico che offrono nuovi spunti di riflessione per il giurista.

La prima non può che essere rivolta ai "pratici", ossia a coloro che ricorrono all'uso degli evoluti sistemi di intercettazione e controllo quale strumento principale per l'esecuzione delle investigazioni. Posta la loro imprescindibilità nell'accertamento e repressione delle più gravi ed evolute forme di criminalità, non è il loro impiego ad essere oggetto di critica, ma l'abuso[200], ossia il ricorso smodato agli strumenti *de quibus* che, secondo l'originaria *voluntas legis*, avrebbe dovuto rappresentare un'*extrema ratio,* cui ricorrere allorquando gli altri sistemi di investigazione preventiva risultano inefficaci allo scopo perseguito[201]: l'uso "parsimonioso" del mezzo in esame, rispettoso del principio di proporzionalità, potrebbe rappresentare un primo passo per il raggiungimento dell'equilibrio tra sicurezza e diritti individuali.

La seconda considerazione non può che avere come referente chi il sistema politico–criminale lo governa e lo plasma secondo le esigenze contingenti. Non potendo considerarsi *a priori* incostituzionale ogni strumento tecnico attraverso cui realizzare le indagini, occorre che questo sistema venga minuziosamente regolamentato, tenendo conto del bilanciamento tra i vari interessi che possono venire in contrasto.

---

commento alla pronuncia, E. APRILE, *Per la Consulta resta illegittima l'acquisizione del contenuto della corrispondenza epistolare dei detenuti effettuata senza le formalità dell'art. 18* ter *ord. penit.*, in *Cass. pen.*, 2017, p. 1877 ss. Per quanto riguarda la giurisprudenza di legittimità, tra le pronunce più significative, per la portata innovativa dei principi in essa contenuti, Cass., sez. un., 28 luglio 2006, in *Cass. pen.*, 2006, p. 4344 ss. Sul punto, sii rinvia a Cap. II, § ?, nt. ?. Di recente, anche la giurisprudenza di merito sembra aver recepito il *dictum.* Trib. Padova, ord. 15 marzo 2017, in *Dir. pen. cont.*, 29 marzo 2017, con nota di R. FLOR, Data retention *ed art. 132 cod. privacy:* vexata quaestio; nonché annotata da F. RUGGIERI, Data retention *e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 2017, p. 2483 ss.

[199] Sul tema, *ex multis,* R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, cit., p. 1142. Sullo statuto attuale del principio di proporzionalità, si rinvia a C. BONZANO, *Gli accertamenti medici coattivi. Legalità e proporzionalità nel regime della prova*, Padova, 2018, p. 108 ss.

[200] Come sostenuto da Montesquieu, «è un'esperienza eterna che qualunque uomo, che ha un determinato potere, è portato ad abusarne […]. Perché non si possa abusare di un potere, bisogna che, per la disposizione delle cose, il potere arresti il potere. Così MONTESQUIEU, *Lo spirito delle leggi*, Ginevra, 1748, trad. it., Giuffrè, 1989, p. 16.

[201] Se la giurisprudenza europea si mostra parsimoniosa nell'accettare lo strumento in esame, il legislatore nazionale sembra invece enfatizzare il ruolo di questo mezzo di ricerca della prova, quasi a ritenerlo «imprescindibile» nel panorama investigativo. S. BUZZELLI, *Le nuove intercettazioni tra selettività arbitraria e ridimensionamento delle garanzie*, in *Riv. dir. dei media*, n. 2, 2018, p. 5. In sostanza, le intercettazioni devono essere utilizzate solo in casi eccezionali, attraverso un'accurata normativa che detti regole «certe e dettagliate». Corte EDU, Grande Camera, 24 aprile 1990, *Kruslin c. Francia*, cit., § 33. Si vedano, inoltre, Corte EDU, sez. IV, 25 novembre 2003, n. 1303/02, *Lewis c. Regno Unito*, § 19; sez. II, 20 dicembre 2005, *Wisse c. Francia*, cit., § 34; Grande Camera, 10 marzo 2009, n. 4378/02, *Bykov c. Russia*, §§ 69–83. Anche nelle pronunce più recenti la corte conferma il suo rigoroso orientamento. Corte EDU, sez. I, 24 gennaio 2017, n. 64746/14, *Travaglio c. Italia*, § 31.

Inevitabile in questo senso appare l'intervento normativo del legislatore, chiamato a tipizzare il complesso di attività esperibili in fase preventiva in forma chiara e compiuta, in modo da poter avere effettiva cognizione delle modalità di ingerenza degli investigatori alla sfera di riservatezza individuale[202], rendendo così la materia conforme ai principi europei che impongono chiarezza, sufficienza, determinatezza della fattispecie nonché, in particolare, il rispetto del principio di proporzionalità, di modo tale da rendere la limitazioni alla alle prerogative individuali "tollerabili" secondo i parametri propri di una società democratica[203].

[202] Si è da più parti sollecitata una disciplina legislativa, non senza subordinarla comunque alla previa individuazione del relativo fondamento costituzionale e se ne è ricavato l'auspicio che la Corte costituzionale possa procedere al riconoscimento di un nuovo diritto costituzionale alla stregua dell'art. 2 Cost., anziché persistere nell'"errore" di "forzare oltre misura l'interpretazione degli artt. 14 e 15, ritenendo chiusa la lista dei diritti inviolabili", nonostante le perquisizioni online non minaccino né il domicilio né la libertà e segretezza delle comunicazioni. R. ORLANDI, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici,* in *Arch.pen.,* 2016, p. 3.

[203] Sul rispetto di tali *dicta*, *amplius*, R.E. KOSTORIS, *Processo penale e paradigmi europei*, Giappichelli, 2018, p. 153 ss.; G. RANALDI, *Efficacia delle sentenze della Corte EDU e rimedi interni: verso una restitutio in integrum (dal caso Dorigo alla revisione del processo iniquo)*, in AA. VV., *Regole europee e processo penale,* a cura di A. Gaito–D. Chinnici, Wolters Kluwer-Cedam, 2018, p. 27 ss.

CAPITOLO V

IL CAPTATORE INFORMATICO NELLE INDAGINI PROATTIVE

SOMMARIO: 1. La polivalenza funzionale. L'impiego del *Trojan* nelle investigazioni preventive – 2. Le attività intercettive esperibili in fase preventiva – 2.1. *Segue*: oltre i confini della captazione. L'acquisizione dei dati e il tracciamento delle comunicazioni – 3. Intercettazioni preventive e captatore informatico: vuoti normativi e prassi applicative – 4. Il *virus* di Stato quale tecnica di sorveglianza di massa – 4.1 *Segue*: Un'inedita forma di captazione e controllo preventivo: l'*IMSI Catcher* – 5. Le notizie pre–procedimentali come "stimolo" investigativo: le informazioni *ante delictum* serventi la *notitia criminis* – 5.1. *Segue:* I rischi procedimentali delle indagini proattive. La circolazione delle informazioni – 6. L'utilizzabilità processuale del materiale conoscitivo "per" la richiesta di intercettazioni e controlli preventivi – 7. La raccolta preventiva dei dati alla prova dei principi dello Stato di diritto

1. LA POLIVALENZA FUNZIONALE. L'IMPIEGO DEL *TROJAN* NELLE INVESTIGAZIONI PREVENTIVE

A prescindere dall'impiego del *virus* informatico nell'ambito delle intercettazioni "tradizionali", lo strumento in esame manifesta le sue potenzialità anche durante l'espletamento delle investigazioni preventive condotte in un tempo antecedente all'iscrizione della notizia di reato nell'apposito registro.

In altri termini, il *malware* non trova impiego esclusivo nelle indagini di polizia *stricto sensu* intese, venendo ampiamente utilizzato anche nella fase volta all'esplorazione dei dati funzionali alla ricerca della *notitia criminis*: a fronte di un sostanziale mutamento del sistema penale che arretra i suoi argini ad una fase pre-procedimentale[1], il captatore informatico diventa lo strumento privilegiato con il quale gli operatori danno luogo ad intercettazioni e controlli preventivi sulle comunicazioni (art. 226 disp. att. c.p.p.) che, come noto, rappresentano tipici strumenti non propriamente di indagine ma di investigazione, impiegati dalle Forze di polizia e dagli organi di *intelligence* governativa per evitare la commissione di gravi reati di criminalità organizzata e terrorismo[2].

---

[1] Il terrorismo internazionale di matrice islamica e le minacce cybernetiche stanno determinando una trasformazione degli equilibri tra sistema repressivo e preventivo. In questo contesto, il sistema penale sembra che stia rispondendo attraverso un mutamento dei suoi tradizionali connotati ideologici e strutturali (quelli che, da sempre, lo hanno caratterizzato), arrivando a superare l'idea, di matrice retributiva, per cui il suo unico fine è la repressione della fattispecie criminogena attraverso l'accertamento del fatto e la punizione del colpevole. La tendenza più recente è attribuire alla giustizia penale anche una funzione preventiva, di anticipazione del crimine, organizzando la risposta statale secondo modalità, forme e tempi nuovi che allontanano il sistema penale dalla sua immagine tradizionale. Non esiste più, in sostanza, solo il diritto penale della colpevolezza, ma anche (e soprattutto) quello della prevenzione e della neutralizzazione del pericolo, nella convinzione che sia preferibile evitare mali piuttosto che curarli e guarirli. Sul punto, v. D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico*), in *Arch. pen.,* 2016, f. 2, p. 3. Si consenta, inoltre, un rinvio a W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, Wolters Kluwer-Cedam, 2018, p. XI.

[2] In questo senso W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, cit., p. 173 s. Più in generale, sull'istituto delle intercettazioni e dei controlli preventivi sulle comunicazioni, B. AGOSTINI, *La disciplina delle intercettazioni preventive nel sistema antiterrorismo,* in *Dir. pen. cont.,* 2017, f. 1, p. 143 ss.; A. CALÒ, sub *art. 226 disp. att. c.p.p.,* in *Codice*

Ma non solo. Al di là di questa *species* di indagine preventiva, nella prassi investigativa esistono altre forme di sorveglianza anticipata (c.d. "massiva") - esperite quasi esclusivamente mediante l'impiego di sofisticati strumenti informatici - che, pur non trovando espressa regolamentazione, risultano assai utili nella prevenzione del crimine, in quanto indirizzate all'acquisizione di informazioni necessarie a far emergere sospetti che legittimano il compimento delle attività preventive tipizzate ovvero elementi funzionali alla formazione della notizia di reato. Così, le intercettazioni e i controlli preventivi sulle comunicazioni, prodromiche all'acquisizione di informazioni "per" la formazione della notizia di reato, diventano l'immediata conseguenza dell'attività informatizzata di procacciamento dei dati acquisiti su larga scala, "trattati" ed individualizzati allorquando viene percepito un pericolo concreto.

In questo quadro magmatico, gli equilibri di potere tra i protagonisti delle tradizionali indagini preliminari risultano alterati, ingenerando una confusione di ruoli assai "pericolosa": sono gli investigatori (sia Forze di polizia che Servizi d'*intelligence*) a "guidare" le investigazioni e ad orientare il procedimento penale detenendo il monopolio strategico della mole di informazioni raccolte in autonomia e con largo anticipo rispetto all'intervento dell'autorità giudiziaria.

Ciò non senza conseguenze di natura strettamente processuale. La sinergia tra prevenzione e repressione comporta, infatti, il rischio di una convergenza tra organi le cui funzioni sono tradizionalmente separate. Così, l'attività di *intelligence* di raccolta ed elaborazione dei dati acquisiti ai fini di sicurezza diviene ambivalente e, sempre più spesso, attribuita agli organi requirenti (p.m. e p.g.) e, viceversa, le Agenzie di sicurezza si trovano a svolgere attività investigativa che, almeno da un punto di vista teorico, dovrebbe risultare estranea alle stesse.

---

di procedura penale commentato, a cura di A. Giarda–G. Spangher, Wolters Kluwer, II ed., 2001, p. 2545; R. CANTONE–L. A. D'ANGELO, *Una nuova ipotesi di intercettazione preventiva,* in Aa. Vv., *Le nuove norme di contrasto al terrorismo,* a cura di A.A. Dalia, Giuffrè, 2006, p. 54 ss.; A. CAMON, *Le intercettazioni nel processo penale*, Giuffrè, 1996, p. 109 ss.; F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, in Aa. Vv., *Il processo penale tra politiche della sicurezza e nuovi garantismi,* a cura di G. Di Chiara, Giappichelli, 2002, p. 5; L. CERCOLA, *Le intercettazioni nella dinamica del processo penale*, Giappichelli, 2016, p. 460 ss.; G. COLOMBO, *Commento all'art. 226 disp. coord. c.p.p.*, in *Commentario al nuovo codice di procedura penale*, diretto da E. Amodio–O. Dominioni, *Appendice,* a cura di G. Ubertis, Giuffrè, 1990, p. 158; F. DE LEO, *L'irrisolto presente e un possibile futuro delle intercettazioni preventive*, in *Cass. pen.*, 1998, f. 7, p. 1862; R. DINACCI, *Commento all'art. 266 c.p.p.,* in *Codice di procedura penale ipertestuale,* a cura di A. Gaito, Utet, 2001, p. 867; G. DI PAOLO, voce *Prova informatica (diritto processuale penale)*, in *Enc. dir.*, VI, Giuffrè, 2013, p. 748 ss.; L. FILIPPI, *Intercettazioni, tabulati e altre limitazioni alla segretezza delle comunicazioni,* in Aa. Vv., *Procedura penale. Teoria e pratica del processo*, diretto da G. Spangher–A. Marandola–G. Garuti–L. Kalb, Utet, 2015, p. 1118 ss.; ID., *L'intercettazione di comunicazioni,* Giuffrè, 1997, p. 61 ss.; L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, in *Enc. giur.,* XII, Treccani, 2004, p. 2 ss.; G. FUMU, sub *art. 226 disp. att. c.p.p.,* in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, 1992, p. 146 ss.; N. GALLO, *Le intercettazioni e i controlli preventivi sulle comunicazioni,* in *Riv. pol.*, 2008, f. 10, p. 633 ss.; G. MELILLO, *Le recenti modifiche alla disciplina dei procedimenti relativi ai delitti con finalità di terrorismo o eversione*, in *Cass. pen.*, 2002, f. 3, p. 904 ss.; C. MARINELLI, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007, p. 56 ss.; G.G. MEZIO, sub *art. 226 disp. att. c.p.p.*, in *Codice di procedura penale commentato,* a cura di A. Giarda–G. Spangher, Wolters Kluwer, V ed., 2017, p. 1062 ss.; L. PISTORELLI, *Intercettazioni preventive ad ampio raggio ma inutilizzabili nel procedimento penale,* in *Guida dir.*, 2001, f. 42, p. 83 ss.; D. SIRACUSANO–F. SIRACUSANO, *Le prove,* in Aa. Vv., *Diritto processuale penale*, a cura di G. Di Chiara–V. Patanè–F. Siracusano, Giuffrè, 2018, p. 318 ss.; A. VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Cedam, 2011, p. 40 ss.; N. VENTURA, *Sul concetto di intercettazione preventiva di comunicazioni telematiche,* in *Ind. pen.*, 2005, f. 2, p. 559 ss.; A. VIRGILIO, *Il nuovo regime delle intercettazioni preventive,* in *Giust. pen.,* 2002, f. 3, p. 545 ss.

Ci troviamo, così, di fronte ad "nuovo" genere di prevenzione, in cui i confini tra pre-procedimento e indagini sono assai più labili, quasi svaniti ed evanescenti, ricchi di punti di contatto e di scambio. Un concetto di prevenzione 2.0 che, in dispregio ai *dicta* normativi che impongono una netta separazione tra *pre* e *post* procedimento, spinge per una circolazione probatoria di dati ed informazioni e per un'implementazione delle indagini proattive che, inevitabilmente, si ripercuotono sugli esiti procedimentali, sia investigativi che dibattimentali.

2. LE ATTIVITÀ INTERCETTIVE ESPERIBILI IN FASE PREVENTIVE

Le intercettazioni preventive, «meno note agli addetti al settore, ma pur sempre esistenti nel sistema giuridico penale»[3], sono definite come attività tecniche eseguite per esclusive finalità investigative ed assolutamente inutilizzabili nel procedimento penale, ovvero come «un'attività di iniziativa delle Forze di polizia [nonché dei Servizi d'*intelligence*] diretta a raccogliere informazioni utili per la prevenzione di gravi reati e non per l'acquisizione di elementi finalizzati all'accertamento della responsabilità per singoli fatti delittuosi»[4].

In relazione all'individuazione del contenuto dell'attività intercettiva, l'art. 226, comma 1 disp. att c.p.p. prevede la possibilità di procedere all'«intercettazione di comunicazioni o conversazioni, anche per via telematica, nonché all'intercettazione di comunicazioni o conversazioni tra presenti anche se queste avvengono nei luoghi indicati dall'art. 614 c.p.»; inoltre, a norma del comma 4, può essere autorizzato il «tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione dei dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni»[5].

Dunque, dal combinato disposto dai commi 1 e 4 dell'art. 226 disp. att. c.p.p. si evince che le *species* di attività esperibili attraverso il ricorso all'istituto in esame non possono ritenersi limitate alla sola captazione di flussi di dati (c.d. intercettazioni preventive *strictu sensu*), ma si spingono fino a ricomprendere l'acquisizione di ogni altra informazione utile alle investigazioni pre–procedimentali (c.d. controlli preventivi sulle comunicazioni).

Lasciando ad un momento successivo la disamina delle "altre" modalità di acquisizione dei dati, *prima facie* si può ritenere che le operazioni captative eseguibili in sede preventiva ricalchino

---

[3] Così M. DI STEFANO–B. FIAMMELLA, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (Profili di* intelligence), Altalex, 2015, p. 31 ss.

[4] In questo senso, R. CANTONE–L. A. D'ANGELO, *Una nuova ipotesi di intercettazione preventiva,* in Aa. Vv., L*e nuove norme di contrasto al terrorismo,* a cura di A.A. Dalia, Giuffrè, 2006, p. 54. Altri le definiscono come «le interferenze nella segretezza delle comunicazioni la cui finalità non è quella di costituire un mezzo di ricerca della prova nell'ambito di un procedimento penale, ma di agevolare l'attività di prevenzione dei reati». Così M.L. DI BITONTO, *Terrorismo internazionale. Procedura penale e diritti fondamentali in Italia*, in *Cass. pen*., 2012, f. 3, p. 1196. Nello stesso senso anche F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 4; L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 1; F. RUGGIERI, *D.l. 18 ottobre 2001, n. 374, convertito con modificazioni in l. 15 dicembre 2001, n. 438 – Disposizioni urgenti per contrastare il terrorismo internazionale. Commento all'art. 5 (Intercettazioni preventive),* in *Legislaz. pen*., 2002, p. 795.

[5] Come precisa G.G. MEZIO, sub *art. 226 disp. att. c.p.p*., cit., p. 1065, «[O]ggetto di autorizzazione può essere tanto l'intercettazione di comunicazioni a distanza, anche per via telematica, che tra presenti, ancorché queste si svolgano nel domicilio». Dal disposto si deduce che oggetto dell'attività captativa sono tutte le conversazioni o comunicazioni, anche se effettuate per via telematica, mentre si ritiene che non possano essere ricomprese quelle di cui all'art. 103, comma 5 c.p.p., ovvero quelle dei difensori, degli investigatori privati autorizzati, dei consulenti tecnici e loro ausiliari, né quelle tra gli stessi e le persone assistite.

in toto quelle attuabili in fase repressiva: in sostanza, possono essere autorizzate – *ante delictum* – intercettazioni di flussi di comunicazioni o conversazioni telefoniche, ambientali, domiciliari e telematiche.

La possibilità di adattare le attività esperibili nel corso del procedimento penale anche ad uno stadio *extra* processuale determina profili di criticità in termini di tenuta costituzionale della normativa.

In relazione alle intercettazioni preventive domiciliari, si rileva che il dettato normativo dell'art. 226 disp. att. c.p.p. non prevede alcuna condizione supplementare nel caso di captazioni che avvengono nei luoghi di privata dimora[6]: soluzione normativa gravemente dubbia sotto il profilo di compatibilità con l'art. 14 Cost., «dal momento che alla violazione del diritto di comunicare segretamente si affianca, in tale ipotesi, una gravissima violazione dell'intimità domiciliare, non disciplinata dalla legge»[7].

Va comunque precisato che, sia pur con riferimento alla disciplina delle intercettazioni domiciliari processuali previste per procedimenti di criminalità organizzata, secondo un orientamento giurisprudenziale pressoché unanime, la normativa di cui all'art. 13 del d.l. 152/1992 «non contrasta con il disposto dell'art. 14 Cost., nella parte in cui non stabilisce i modi in cui può avvenire la limitazione dell'inviolabilità del domicilio, in quanto tale diritto deve essere correlato alla possibilità di compressione consentita dalla norma costituzionale di cui all'art. 15 Cost. nelle forme delle ispezioni, perquisizioni e sequestri. Ne consegue che, anche in materia di intercettazione di comunicazioni, deve ritenersi applicabile la limitazione per il concreto soddisfacimento di interessi pubblici; inoltre, la riserva di legge appare rispettata dalla dettagliata disciplina prevista dal codice di procedura penale per le intercettazioni di comunicazioni anche tra presenti»[8].

Ma il *dictum* non può trovare immediata applicazione nell'ambito delle intercettazioni domiciliari preventive, in quanto, come noto, il dettato normativo di cui all'art. 226 disp. att. c.p.p. non risulta così rigoroso e dettagliato come quello che disciplina le intercettazioni processuali.

---

[6] Circa la definizione di "luoghi di privata dimora", da ultimo, Cass., sez. un., 23 marzo 2017, n. 31345, in *Dir. pen. cont.,* n. 7–8, 2017, con nota di S. BERARDI, *Le Sezioni Unite ridefiniscono la nozione di privata dimora ai fini dell'art. 624* bis *c.p.,* ritenendo che «rientrano nella nozione di privata dimora di cui all'art. 624–*bis* c.p. esclusivamente i luoghi, anche destinati ad attività lavorativa o professionale, nei quali si svolgono non occasionalmente atti della vita privata, e che non siano aperti al pubblico né accessibili a terzi senza il consenso del titolare». Stante il maggior grado di riservatezza presumibilmente esistente, in caso di intercettazioni "tradizionali", qualora la captazione *inter praesentes* avvenga nei luoghi di cui all'art. 614 c.p., questa è consentita solo allorquando vi sia fondato motivo di ritenere che in quel luogo si stia consumando un'attività criminosa; requisito, di contro, non richiesto né nell'ambito di procedimenti di criminalità organizzata, minaccia col mezzo del telefono, delitto di assistenza agli associati, nonché dei delitti di cui all'art. 407 comma 2, lett. *a*, n. 4 c.p.p. (*ex* art. 13, d.l. 13 maggio 1991, n. 152), né nel caso di intercettazioni preventive. Sul punto, si rinvia a Cap. II, §?.

[7] Si esprime così F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 16 s. Nello stesso senso, L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 7; G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, in *Dir. pen. proc*., 2005, f. 12, p. 1458. *Contra*, G.G. MEZIO, sub *art. 226 disp. att. c.p.p*., cit., p. 1065, secondo cui «[…] il livello di protezione originariamente accordato alla libertà di comunicare segretamente è […] reputato idoneo a garantire la tutela della libertà domiciliare riconosciuta dall'art. 14 Cost. Tanto in forza di una scelta legislativa che non parrebbe azzardato definire contraddistinta da profili di irragionevolezza, attesa la lampante diversità di trattamento rispetto alla corrispondente disciplina delineata dalle norme del codice, dove, la possibilità di disporre lo svolgimento di intercettazioni nel domicilio è assistita da un *surplus* di garanzia».

[8] Così Cass., sez. VI, 21 gennaio 2004, n. 6071, in *Cass. pen*., 2005, f. 12, p. 3926 ss. Nello stesso senso, *ex multis,* sez. IV, 28 settembre 2005, n. 47331, in *C.E.D. Cass.*, n. 232777; sez. I, 2 ottobre 2007, n. 38716, *ivi*, n. 238108. *Contra*, sez. III, 11 giugno 2003, n. 38716, *ivi*, n. 224894.

Per tali ragioni, stante il silenzio del legislatore su questa peculiare ipotesi di captazione preventiva, potrebbe risultare alquanto dubbia la compatibilità della norma con il principio della riserva di legge di cui all'art. 15 Cost.

Altrettanto problematica è la trasferibilità, in fase preventiva, della disciplina delle intercettazioni telematiche processuali di cui all'art. 266 *bis* c.p.p.

La *quaestio* deriva dall'inciso contenuto nel comma 1 dell'art. 226 disp. att. c.p.p., che consente captazioni *ante delictum* di comunicazioni o conversazioni effettuate «anche per via telematica»[9].

In questo caso la norma, a differenza dell'omologa fattispecie processuale, non fa alcun richiamo ai "flussi di comunicazioni intercorrenti tra più sistemi" e nemmeno ai "flussi di comunicazioni relativi a sistemi informatici": non riproducendo *in toto* il disposto dell'art. 266 *bis* c.p.p., si è ritenuto che il legislatore non abbia voluto introdurre la possibilità di esperire, in fase preventiva, le intercettazioni telematiche e, «poiché l'art. 226 disp. att. c.p.p. comprime un diritto fondamentale dell'individuo […] sembra difficile ritenere che lo strappo normativo possa essere ricucito in sede esegetica»[10].

L'interpretazione rigorosa del dettato normativo, tuttavia, desta non poche perplessità, in quanto la voluta espansione della portata delle intercettazioni preventive a tutte le *species* di captazioni[11] sembra stridere con l'opposta tendenza di escludere quelle informatiche o telefoniche, conflitto che si acuisce allorquando ci si confronta con il disposto del comma 4 del medesimo articolo che consente, *de facto*, di esperire nella fase *extra* procedimentale tutta una seria di attività che si spingono ben oltre la mera apprensione di flussi comunicativi.

Si potrebbe, allora, ipotizzare che la laconicità del dettato di cui all'art. 226 disp. att. c.p.p. sia il frutto di una "svista" legislativa piuttosto che di una consapevole scelta di indirizzo normativo, colmabile in sede interpretativa; né parrebbe altrimenti ipotizzabile in ragione dell'esplicito rinvio alle comunicazioni realizzate «anche per via telematica», richiamo che, peraltro, consente di garantire la tenuta costituzionale della restrizione del diritto alla segretezza di ogni forma comunicativa che può avvenire, a norma dell'art. 15 Cost., solo se espressamente prevista dalla legge.

---

[9] L'infelice formulazione della norma si deve ad un difetto di coordinamento tra il testo originario del decreto legge e il testo approvato in sede di conversione. Cfr. l'intervento del senatore Bobbio, in *Atti Senato*, XIV leg., seduta del 6 dicembre 2001.

[10] Si esprime così F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 16, il quale aggiunge che «[È]è vero che l'inciso "anche per via telematica" è preceduto da un richiamo apparentemente onnicomprensivo alle "comunicazioni" a distanza, ma l'art. 5 comma 3 del decreto legge, occupandosi di impianti utilizzati per le operazioni di ascolto, allude ugualmente alle intercettazioni telefoniche o telematiche». Sul tema, esaustivamente, veda anche, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018, p. 300, secondo cui «per espressa indicazione dell'art. 226, comma 1 disp. att. c.p.p. le intercettazioni preventive possono essere effettuate anche in via telematica».

[11] Si allude all'inserimento, in fase di conversione, della possibilità di eseguire intercettazioni preventive *inter praesentes*. Più precisamente, il riferimento alle «intercettazioni di comunicazioni o conversazioni tra presenti, anche se avvengono nei luoghi indicati dall'art. 614 c.p.» è stato inserito in sede di conversione in legge del d.l. 374/2001, con ciò ampliando l'ambito operativo delle intercettazioni preventive anche a quelle ambientali.

2.1. OLTRE I CONFINI DELLA CAPTAZIONE. L'ACQUISIZIONE DEI DATI E IL TRACCIAMENTO DELLE COMUNICAZIONI

Come anticipato, il complesso di attività rientranti nel *genus* delle intercettazioni preventive non si esaurisce nella mera captazione di conversazioni o comunicazioni, finendo per ricomprendere l'acquisizione di qualsivoglia dato utile all'investigazione pre–procedimentale.

In alternativa o congiuntamente alle intercettazioni, ai sensi del comma 4 dell'art. 226 disp. att. c.p.p., si prevede che «con le modalità e nei casi di cui ai commi 1 e 3, può essere autorizzato il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione di dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni»[12], regolamentando tre differenti tipologie di atti già utilizzati nella prassi ma che mai prima d'ora erano stati oggetto di esplicita menzione da parte del legislatore[13].

Il riferimento espresso alla disciplina contenuta nei commi 1 e 3 dell'art. 226 disp. att. c.p.p. ha come conseguenza che i medesimi soggetti legittimati a chiedere le intercettazioni preventive possono domandare al pubblico ministero funzionalmente competente l'autorizzazione al controllo preventivo dell'utenze appartenenti al soggetto monitorato nell'ipotesi in cui ciò appaia necessario al fine di assumere notizie utili per la prevenzione dei delitti di cui agli artt. 407, comma 2 lett. *a*, n. 4 e 51, commi 3 *bis* e *quater* c.p.p.

Al di là delle discutibili scelte stilistiche del dettato normativo, occorre chiarire la portata investigativa dei due strumenti al fine di verificare la compatibilità dei sistemi di sorveglianza con il sostrato costituzionale.

In primo luogo, va detto che, pur differenziandosi per aspetti squisitamente tecnici, il "tracciamento delle comunicazioni" e l'"acquisizione dei dati esterni"[14] (c.d. tabulati)[15]

---

[12] I dati relativi al traffico telefonico devono essere tenuti distinti da quelli inerenti alle comunicazioni telematiche o informatiche. Le comunicazioni telefoniche, consentono la ricetrasmissione di dati attraverso la linea telefonica, mentre quelle telematiche si sostanziano nello scambio di informazioni tra elaboratori elettronici mediante canali alternativi, siano essi il collegamento via cavo, intranet o etere. Cfr. E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche e ambientali*, Giuffrè, 2004, p. 104. Si veda, inoltre, L. D'ANGELO, *La conservazione dei dati del traffico*, in Aa. Vv., *Le nuove norma di contrasto al terrorismo*, cit., p. 159 ss.

[13] L. FILIPPI, *Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali*, in *Dir. pen. proc*., 2002, f. 2, p. 168. Sul tema, approfonditamente F. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito di tabulati, tracciamenti, intercettazioni, conservazioni di dati e dintorni*, in *Cass. pen*., 2002, f. 12, p. 2208 ss. Più di recente, T. BENE, *Il pedinamento elettronico: tecnica di investigazione e tutela dei diritti fondamentali,* in AA. VV., *Le indagini atipiche*, a cura di A. Scalfati, Giappichelli, 2019, II ed., p. 443; F.R. DINACCI, *La localizzazione mediante celle telefoniche tra limiti costituzionali e comunitari*, *ivi,* p. 465 ss.

[14] Il carattere "esterno" delle comunicazioni si contrappone a quello "interno" avente ad oggetto il contenuto delle comunicazioni. Cfr. E. APRILE–F. SPIEZIA, *Le intercettazioni telefoniche e ambientali*, cit., p. 104; M. DE BELLIS, *La disciplina della acquisizione dei tabulati telefonici nel suo sviluppo normativo e giurisprudenziale*, in *Arch. n. proc. pen*., 2008, p. 26.

[15] Il tabulato può essere definito come un «prospetto, originariamente stampato su carta, come suggerisce l'etimo del sostantivo, ma sempre più spesso memorizzato su supporto digitale, contente i c.d. dati esterni traffico telefonico e telematico». Cfr. N. ZINGARELLI, voce *Tabulato*, in *Vocabolario della lingua italiana*, Zanichelli, 2018. In senso tecnico, «con il termine dati esterni di una comunicazione vengono indicati quei dati che permettono di instradare una comunicazione dal richiedente al destinatario […]. Nel caso della telefonia fissa questi dati sono il numero telefonico del chiamante, quello del chiamato e il tempo di inizio e fine della chiamata […]. Nel caso di una comunicazione tramite telefonia mobile, le informazioni relative all'utente chiamato, al chiamante, al tipo di servizio richiesto, all'avvenuta risposta, alla posizione geografica in cui può essere raggiunto l'utente mobile, sono necessarie a costruire e veicolare la comunicazione e per la tariffazione della

condividono la medesima finalità, ovvero lo "spionaggio" e il controllo delle svariate attività che gli utenti dei servizi di telefonia o della rete compiono nella quotidianità e la presa di conoscenza dei soli dati attinenti al fatto storico del contatto telefonico o telematico, della durata e del volume del traffico nonché della posizione degli apparati, in quanto nessuno dei dei due strumenti consente l'apprensione del contenuto delle conversazioni effettuate.

Inoltre, i due strumenti condividono la mancanza di simultaneità tra ciò che accade e ciò che si apprende: la non contestualità della captazione del contenuto dei flussi comunicativi è un dato che rimarca le differenze esistenti tra queste forme di controllo preventivo e la disciplina delle intercettazioni *ante delictum*[16]. Infatti, mentre quest'ultima consiste in un'occulta presa di conoscenza contestuale del contenuto di una conversazione *inter praesentes* o *absentes*, sia il tracciamento delle comunicazioni che l'acquisizione dei tabulati intervengono *ex post* e in modo apparentemente non insidioso, prescindendo anche dall'impiego di dispositivi tecnici che, di contro, sono essenziali nella disciplina delle intercettazioni[17].

In effetti, la linea di demarcazione tra le operazioni di controllo e quelle di intercettazione – sia pur con riferimento a quelle giudiziarie – è già stata evidenziata a più riprese dalla giurisprudenza di legittimità, secondo cui «[…] l'individuazione dell'utenza di provenienza delle telefonate non integra un'attività di intercettazione […], bensì un mero accertamento di fatto riconducibile alla generica attività di assicurazione delle fonti di prova che la p.g. può svolgere anche di propria iniziativa»[18]; anche la Consulta sostiene l'impossibilità di accomunare le due

---

chiamata […]. I dati memorizzati riguardano la totalità delle comunicazioni mobili e possono essere utilizzati a posteriori per verificare gli spostamenti degli individui sottoposti ad indagini». Così A. PAOLONI–D. ZAVATTARO, *Intercettazioni telefoniche e ambientali*, Centro Scientifico Editore, 2007, p. 98. Sulla nozione dei tabulati telefonici anche, M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, in *Dir. pen. cont*., 9 dicembre 2016, p. 156 ss.

[16] Sulle differenze esistenti tra le nozioni di flussi comunicativi e dati esteriori, si rinvia a C. SCACCIANOCE, *Approvvigionamento di flussi e dati tramite il dispositivo elettronico altrui*, in Aa. Vv., *Le indagini atipiche,* a cura di A. Scalfati, I ed., 2015, p. 35 ss.

[17] In questo senso F. CAPRIOLI, *Colloqui riservati e prova penale*, Giappichelli, 2000, p. 172. Ne rimarca le differenze anche L. FILIPPI, *Intercettazioni, tabulati e altre limitazioni alla segretezza delle comunicazioni*, cit., p. 971 s. Come sottolinea F. DE LEO, *Controllo delle comunicazioni*, cit., p. 2214, «l'intercettazione è la captazione di una comunicazione in corso, è ad essa contemporanea; l'acquisizione di un tabulato è l'apprensione di un dato storico, di un fatto che è stato e che in un momento successivo viene rappresentato in un documento. Non si può estendere a una situazione statica una disciplina nata per regolamentare una situazione in movimento. L'incompatibilità quindi non dipende dal grado di invasività dell'atto di indagine (che può anche esserci ma è irrilevante ai fini della pertinenza normativa) ma è logica, dipendendo dalla modalità e dalla temporalità con le quali l'atto si compie. Ma i dati esterni alla comunicazione possono essere non solo raccolti quando ormai la comunicazione è avvenuta da tempo, e quindi sotto forma di documento, ma possono anche essere colti in contemporanea alla comunicazione». Nello stesso senso anche F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 28. Deve, tuttavia, ritenersi che la simultaneità è caratteristica propria del solo sistema di tracciamento mediante GPS e non anche mediante localizzazione attraverso celle telefoniche. La simultaneità dell'apprensione è anche caratteristica propria del c.d. "tracciamento AXE" (dal nome delle centrali Ericsson utilizzate da alcuni operatori di telecomunicazioni) che rappresenta l'evoluzione di quella che, con le vecchie centrali elettromeccaniche, si chiamava «blocco» della chiamata: attraverso il «blocco» – cioè l'arresto degli organi di commutazione su tutta la rete – si poteva materialmente seguire il tracciato della comunicazione all'interno della rete stessa e così individuare la linea del soggetto chiamante.

[18] Cass., sez. II, 7 ottobre 1998, n. 8248, in *Giur. it.,* 1999, p. 1687, con nota di L. FILIPPI. Sul punto anche M. VIALI, *L'acquisizione dei dati "esteriori" di conversazioni o comunicazioni: tra nuove tecnologie e sbandamenti giurisprudenziali*, in *Cass. pen*., 1999, f. 9 p. 2576 ss. Cfr., anche, Cass., sez. un., 8 maggio 2000, n. 6, in *Cass. pen.,* 2000, f. 12, p. 3235, con nota di L. FILIPPI, *Il* revirement *delle Sezioni unite sul tabulato telefonico: un'occasione mancata per riconoscere una prova incostituzionale.*

attività, ritenendo che «i "dati esteriori" delle comunicazioni non costituiscono oggetto di un'intercettazione in senso tecnico, con conseguente inoperatività della disciplina prevista per quel mezzo di ricerca della prova»[19].

Ad ogni modo, a prescindere dall'impossibilità di ricondurre suddette attività nell'alveo delle captazioni *ante delictum*, il legislatore decide scientemente di estendere alle stesse il sistema generale predisposto per le intercettazioni preventive, sottoponendole al vaglio autorizzativo del pubblico ministero[20].

Nonostante le similitudini operative e sistemiche tra i due strumenti, va evidenziato che il rapporto che lega gli strumenti di controllo in esame è di specie a genere: il "tracciamento delle comunicazioni" rappresenta solo una delle molteplici attività che possono essere compiute mediante l'acquisizione dei tabulati telefonici.

Detto in altri termini, le informazioni apprese mediante il *tracking* delle comunicazioni rappresentano solo una piccola porzione della mole di dati ottenibili attraverso l'apprensione dei prospetti contenenti i dati esterni alle comunicazioni[21].

Per quanto concerne il c.d. "tracciamento delle comunicazioni", esso consiste nel «sottoporre a controllo l'utenza intercettata per rilevarne gli spostamenti nello spazio»[22].

---

[19] Corte cost., 11 marzo 1993, n. 81, in *Cass. pen*, 1993, f. 9, p. 2741, con nota di D. POTETTI, *Corte costituzionale n. 81/93: la forza espansiva della tutela accordata dall'art. 15 comma 1 della Costituzione*; in *Giur. cost.,* 1993, p. 731, con nota di G.P. DOLSO, *Ipotesi sulla possibilità di un diverso esito utilizzando il parametro della «ragionevolezza»* e p. 2111 con nota di A. PACE, *Nuove frontiere della libertà di «comunicare riservatamente» (o, piuttosto, del diritto alla riservatezza)?*; in *Giur.it.,* 1995, p. 108, con nota di S. DI FILIPPO, *Dati esteriori delle comunicazioni e garanzie costituzionali.* Con un successivo intervento la Consulta, dopo aver ribadito che la disciplina dei tabulati è attratta nella garanzia prevista dall'art. 15 Cost., ha rilevato l'impossibilità di una sentenza additiva che estendesse la disciplina delle intercettazioni all'acquisizione del tabulato, formulando un espresso invito al legislatore affinché «provvedesse a disciplinare in modo organico l'acquisizione […] della documentazione relativa al traffico telefonico […]». Così Corte cost., 17 luglio 1998, n. 281.

[20] La norma prosegue stabilendo che elle operazioni svolte e dei contenuti intercettati viene redatto verbale sintetico che, unitamente ai supporti utilizzati, deve essere depositato, nel termine di cinque giorni dall'esecuzione delle stesse, presso la segreteria del pubblico ministero che ha autorizzato il compimento delle attività. Allorquando il pubblico ministero verifichi la corrispondenza tra l'autorizzazione emessa e le operazioni compiute, deve disporre l'immediata distruzione dei supporti e dei verbali, in analogia a quanto accade in tema di intercettazioni preventive. Favorevole all'inquadramento sistematico prescelto dal legislatore, F. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito dei tabulati, tracciamenti, intercettazioni, conservazione di dati e dintorni),* cit., p. 2217, secondo cui «[..]qui non solo per la prima volta affiora in un testo legislativo il concetto di tracciamento ma esso viene correttamente riportato sotto il paradigma delle intercettazioni». Si soffermano sulle attività *de qua*, F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 27 ss.; L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 9; L. FILIPPI, *Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali*, cit., p. 168 s.; G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, cit., p. 1461.

[21] La «forte idoneità intrusiva» dei tabulati telefonici è stata sottolineata dalla Corte costituzionale, soprattutto in relazione al fatto che, nella misura in cui si riferiscono ad utenze "mobili", gli stessi, oltre ad indicare il dato storico della comunicazione e dei relativi tempi di durata, sono in grado di individuare i luoghi in cui si trova il soggetto della cui utenza si è acquisito il tabulato. Cfr. Corte cost., 28 maggio 2010, n. 188, *in www.cortecostituzionale.it.* Sulle differenze tra le due attività, F. DE LEO, *Controllo delle comunicazioni e riservatezza (a proposito dei tabulati, tracciamenti, intercettazioni, conservazione di dati e dintorni),* cit., p. 2214 s. Sul tema, anche, M. DI STEFANO–B. FIAMMELLA, *Intercettazione: remotizzazione e diritto di difesa nell'attività investigativa*, cit., p. 224 ss.

[22] Così L. FILIPPI, sub *art. 266,* cit., p. 2606. Sulla ricostruzione degli spostamenti di un soggetto attraverso l'analisi delle celle telefoniche agganciate sul traffico telefonico e telematico, S. ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale,* in *Giur. merito*, 2013, f. 4, p. 955

L'attività in esame risulta, allo stato, espressamente normata: l'art. 126 del Codice per la *privacy* consente al gestore del servizio di comunicazione, entro certi limiti, di trattare i dati relativi all'ubicazione del terminale mobile anche se diversi dai dati inerenti al traffico, permettendo agli inquirenti di richiedere allo stesso il "futuro" tracciamento dell'utenza per verificare gli spostamenti sul territorio.

Il *tracking* delle comunicazioni avviene grazie all'ausilio delle c.d. celle telefoniche (*rectius* torre radio) cui è agganciata l'utenza. Quando un apparecchio telefonico si sposta nel territorio da una torre–radio ad un'altra deve rinegoziare la connessione con la rete telefonica e, quindi, diventa ricostruibile il suo movimento anche in assenza di chiamata (*call site analysis*)[23].

Dunque, nel prendersi atto che il tracciamento delle comunicazioni può effettuarsi attraverso l'individuazione delle celle telefoniche in cui viene agganciata l'utenza, la localizzazione del soggetto può agevolmente effettuarsi tramite l'acquisizione di un tabulato telefonico da cui è possibile ricavare ogni spostamento dell'individuo detentore dell'apparecchio[24].

Se così stanno le cose, l'acquisizione del tabulato telefonico rappresenta un *quid pluris* rispetto al semplice tracciamento delle comunicazioni, dal momento che consente l'apprensione di un ventaglio di informazioni assai più ampio e variegato che finisce anche con il ricomprendere la mappatura degli spostamenti dell'utenza mobile.

Tuttavia, il *tracking* di un soggetto attraverso il monitoraggio del dispositivo mobile in suo possesso è realizzabile con diverse modalità operative che consentono, *de facto*, di bypassare l'intermediazione del gestore del servizio e, conseguentemente, di accelerare i tempi di indagine.

Si tratta, in sostanza, di un *tracking* satellitare il cui oggetto non è la persona o il veicolo, ma il dispositivo mobile del monitorato, sfruttando il sistema di posizionamento geografico GPS (*Global Positioning System*) in grado di rilevare, in tempo reale, le coordinate spazio–temporali in qualsiasi punto esso si trovi[25].

La possibilità di monitorare il soggetto si realizza, dunque, tramite l'attivazione, da remoto, del localizzatore satellitare di cui dispongono i più moderni dispositivi elettronici portatili: detto sistema consente non solo di stare al passo con la "frenesia investigativa", ma anche di avere informazioni in tempo reale, nello stesso momento in cui si sta consumando lo spostamento spaziale. Ad ogni modo, il sistema "fai da te" non sembra immune da contraccolpi: mancando l'apporto del gestore del servizio e appare assai verosimile il rischio, soprattutto in fase preventiva, di intercettazioni abusive.

Tra le altre attività esperibili in sede di monitoraggio *ad personam*, il legislatore annovera anche la possibilità di acquisire «ogni altra informazione utile in possesso degli operatori di telecomunicazioni».

Il disposto, sempre eccessivamente vago e assai generico, determina, almeno in potenza, il rischio di legittimare qualsivoglia attività funzionale all'apprensione di notizie utili alle investigazioni *ante delictum*. Questa sorta di "norma penale in bianco", potrebbe causare una

---

ss.

[23] Così F.R. DINACCI, *La localizzazione mediante celle telefoniche tra limiti costituzionali e comunitari*, cit., II ed., p. 465. Circa l'attendibilità dello strumento, A. CACCAVELLA, *Attendibilità dei tabulati telefonici*, in *Dir. dell'internet,* 2007, p. 95 ss. In tema anche, N. BASSETTI–P. REALE, *I dati telefonici per finalità giudiziarie nelle applicazioni reali,* in *Sicurezza e giustizia*, 2014, f. 1, p. 47 ss.

[24] Qualora un utente telefonico le cui abitudini in termini di quantità di SMS o conversazioni sono piuttosto contenute, riflettendosi in limitatissime (se non addirittura assenti) tracce sui tabulati, è però possibile che questi stia utilizzando un terminale di ultima generazione, uno *smartphone*, che fa generoso accesso alla rete di tipo "dati" per la consultazione della posta elettronica, per le notifiche di *Facebook*, per i messaggi di *WhatsApp* e così via. Ciò si traduce in un tabulato telematico di indubbio interesse investigativo, poiché spesso tali connessioni hanno maggiore frequenza e continuità temporale.

[25] Sul pedinamento elettronico mediante GPS satellitare, si consenta un rinvio a Cap. II, § ?.

violazione del principio della riserva di legge disposto dell'art. 15 Cost., non specificando i "casi" in cui la compressione del diritto alla libertà e alla segretezza della corrispondenza può essere compresso.

Passate in rassegna tutte le attività – intercettive o di controllo delle comunicazioni– che possono essere esperite in fase preventiva, a norma dell'art. 226 disp. att. c.p.p., un dato resta ancora ignoto.

Esiste, infatti, una vasta gamma di attività di "monitoraggio della persona" che, non essendo in alcun modo disciplinata dal legislatore, sono definibili come "indagini preventive atipiche"[26], il cui esperimento determina non poche conseguenze sul versante processuale dal momento che, a precise condizioni, i relativi dati acquisiti possono fare ingresso nel corso del procedimento, favorendo il processo di osmosi probatoria tra *pre* e *post notitia criminis*[27].

3. Intercettazioni preventive e captatore informatico: vuoti normativi e prassi applicative

Per quanto concerne l'impiego del captatore informatico in fase preventiva, il nervo scoperto della materia si rivela nell'assenza di regole atte a disciplinare la peculiare attività per esperire le intercettazioni e i controlli preventivi sulle comunicazioni: l'aggiornamento normativo che di recente ha colpito l'istituto delle intercettazioni giudiziarie[28], non intacca l'istituto esperibile *ante delictum*[29].

Stante l'incidenza sul piano dei diritti fondamentali di una simile tecnica investigativa[30], parrebbe necessario limitarne il più possibile la sfera operativa, restringendo il campo di azione

---

[26] Si pensi al pedinamento elettronico, allo spionaggio informatico, alla sorveglianza *online*. Per una panoramica delle attività investigative atipiche svolte sia in fase repressiva ma che trovano compiuta realizzazione anche in fase preventiva, più di recente, E. APRILE, voce *Captazioni atipiche (voci, immagini, segnali)*, in *Dig. proc. pen.* on line, diretto da A. Scalfati, Giappichelli, 2012; S. ATERNO–M. MATTIUCCI, *Il* Cloud forensics *e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.,* 2013, f. 3, p. 865 ss.; F. CAJANI, *Le operazioni digitali sotto copertura: l'agente provocatore e l'attività di contrasto nelle indagini informatiche,* in Aa. Vv., Computer forensics *e indagini digitali. Manuale tecnico–giuridico e casi pratici*, a cura di S. Aterno–F. Cajani–C. Costabile–M. Mattiucci–G. Mazzaraco, Experta editore, 2011, p. 411 ss.; C. CONTI–M. TORRE, *Spionaggio digitale nell'ambito dei* social network, in AA. VV., *Le indagini atipiche*, II ed., cit., p. 535 ss.; P. FELICIONI, *Le fattispecie "atipiche" e l'impiego processuale,* in AA. VV., *L'intercettazione di comunicazioni*, a cura di T. Bene, Cacucci, 2018, p. 303 ss.; D. GENTILE, *Il* Tracking satellitare *mediante GPS: attività atipica di indagine o intercettazione di dati,* in *Dir. pen. proc.,* 2010, p. 1464 ss.; E.M. MANCUSO, *La perquisizione* on–line, in *Jus*, 2017; G. DI PAOLO, "*Tecnologie de controllo" e prova penale. L'esperienza statunitense e spunti per la collaborazione*, Cedam, 2008, *passim*; L. PARLATO, *Problemi insoluti: le perquisizioni* on-line, in AA. VV., *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di G. Giostra-R. Orlandi, Giappichelli, 2018, p. 289 ss.; EAD., voce *Perquisizioni* on line, in *Enc. dir.*, Annali, X, Giuffrè, 2017, p. 601 ss.; S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi*, in *Riv. it. dir. proc. pen.,* 2012, f. 2, p. 580 ss.; M. STAMAGLIA, *Il pedinamento satellitare: ricerca ed uso di una prova atipica*, in *Dir. pen. proc.*, 2011, f. 2, p. 213 ss.

[27] Sul tema, si rinvia a § ?.

[28] Cfr. d.lgs. 216/2017 e successive modifiche. Sul tema, v. *amplius* Cap. 1.

[29] Una simile lacuna viene avvertita da R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, f. 2, p. 544 s., il quale precisa che «[L]la riforma del 2017 trascura del tutto il delicato ambito delle intercettazioni preventive».

[30] Proprio come accade per le intercettazioni "giudiziarie", la possibilità di monitorare da remoto, segretamente e senza limiti spazio–temporali, ogni attività che il soggetto conduce, importa evidenti

alle sole intercettazioni "giudiziarie" come espressamente previsto dal legislatore: la mancanza di una previsione volta a legittimare l'impiego del captatore informatico in riferimento alle intercettazioni preventiva «potrebbe suonare come un'esclusione»[31].

Una simile impostazione, tuttavia, non convince del tutto l'interprete.

Intanto, nel caso in esame non pare ipotizzabile il riferimento al canone *ubi lex voluit, dixit; ubi noluit, tacuit*. E ciò per due ordini di ragioni.

In primis, il silenzio del legislatore in tema di captatore informatico per le intercettazioni preventive non pare in alcun modo probante, «perché l'orizzonte preventivo sembra eccedere i limiti previsti dalla legge delega 103/2017 che aveva infatti ad oggetto solo modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario e non anche alle norme in tema di prevenzione»[32].

In secondo luogo, l'assenza di previsioni espresse nel dettato normativo non ha rappresentato motivo di esclusione di attività che, secondo un'interpretazione rigorosa del *dictum*, sembrano illecite.

Si pensi all'incompleto *memorandum* di tipologie di intercettazioni giudiziarie esperibili mediante captatore: come noto, il legislatore decide di tipizzare esclusivamente «l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico», mentre nessun cenno viene fatto alle «comunicazioni informatiche o telematiche»[33], che, *prima facie,* non sembrano essere interessate dalla riforma *de qua.* Tuttavia, la giurisprudenza di legittimità colma il vuoto normativo per via interpretativa attraverso l'inspiegabile ricorso all'*analogia legis*[34], ammettendo comunque l'utilizzo dello strumento anche per condurre intercettazioni informatiche o telematiche[35].

Inoltre, a fronte del richiamo contenuto nel comma 1 dell'art. 226 disp att. c.p.p. alle *species* di intercettazioni esperibili in fase repressiva, appare coerente ammettere l'utilizzo del peculiare

---

collisioni con i diritti costituzionalmente garantiti, quali l'art. 13 Cost., baluardo della libertà di ogni individuo, l'art. 14 Cost., posto a protezione del domicilio, l'art. 15 Cost., che tutela la libertà e la segretezza della corrispondenza e di ogni al–tra forma di comunicazione, nonché, spostando lo sguardo oltre i confini nazionali, il principio di proporzionalità che impone, ai sensi dell'art. 8 CEDU, la necessità di una perfetta corrispondenza tra i risultati perseguiti e i mezzi adoperati e, più in particolare, tra la potenziale forza invasiva del mezzo in esame e l'inevitabile lesione dei diritti fondamentali. Non solo. L'attività *de qua* si pone in contrasto con il rinnovato e più generale diritto alla *privacy* e alla riservatezza, inteso come «presupposto della libertà». Così CGUE, Grande Sezione, 8 aprile 2014, *Digital Rights Ireland e Seitlinger et all.,* cause C–293/12 e C–594/12, §45 ss.

[31] Si esprime così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 301.

[32] Così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa,* cit., p. 301.

[33] Di cui all'art. 266 *bis* c.p.p., ai sensi del quale «Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologia informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

[34] Per una disamina della *quaestio*, v. D. CURTOTTI- W. NOCERINO, *Le intercettazioni tra presenti con captatore informatico*, in AA. VV., *Le recenti riforme in materia penale*, a cura di G.M. Baccari-C. Bonzano-K. La Regina- E.M. Mancuso, Wolters Kluwer-Cedam, 2017, p. 569.

[35] L'utilizzo del captatore informatico non può ritenersi escluso per le intercettazioni tra presenti che trovano luogo nei luoghi di privata dimora dove si sta svolgendo l'attività criminosa e deve ritenersi consentito per l'esecuzione di intercettazioni telematiche, *ex* art. 266 *bis* c.p.p. Così Cass., sez. V, 20 ottobre 2017, n. 48370, cit. Per un commento, C. PARODI, *Intercettazioni telematiche e captatore informatico: quali limiti?*, cit. Sul tema anche S. ATERNO, *La Cassazione, alle prese con il captatore informatico, non convince sull'acquisizione mediante* screen shot, in *Dir. pen. proc.,* 2018, f. 8, p. 1063 ss.

strumento anche in fase preventiva[36]: la recente previsione, infatti, non introduce un nuovo "tipo" di intercettazione, ma delinea l'attività in esame come «una nuova modalità attraverso cui può espletarsi un "vecchio" mezzo di ricerca della prova»[37].

Ne consegue che, pur non essendo espressamente contemplata dalla norma, l'intercettazione preventiva tramite *virus Trojan* sarebbe del tutto legittima in quanto ricompresa implicitamente tra le possibilità della norma stessa, laddove estende la propria sfera operativa a tutte le tipologie di intercettazioni giudiziarie ricomprese nel codice di rito[38].

Per quanto riguarda le "altre" attività che possono essere condotte in via preventiva (quelle di controllo in senso stretto), sembra da escludere la possibilità di utilizzare il captatore informatico.

Pur se potenzialmente in grado di operare un controllo occulto e ad ampio raggio della criminalità, il decreto 216/2017, sembra aver limitato la "portata" del captatore informatico alla mera attività di captazione di conversazioni e comunicazioni: autorizzando la sola attivazione del microfono del dispositivo in cui viene inoculato e inibendo, al contempo, il complesso di attività esperibili con lo strumento in esame[39], il legislatore intende attribuire allo stesso la fisionomia di una "cimice informatica", poco dissimile dalle tradizionali microspie.

Ma se l'unica *species* di captatore "legale" è quella che consente solo di intercettare[40], va da sé che tutte le altre attività esperite a mezzo *Trojan* non possano considerarsi legittime e questo tanto in fase repressiva che preventiva[41].

---

[36] Nello stesso senso, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 304, secondo cui la novella «rende soltanto esplicito il ricorso a una tecnica investigativa che appariva legittima già in precedenza, in quanto modalità di intercettazioni di comunicazioni […]».

[37] Si consenta il richiamo a W. NOCERINO, *Le Sezioni Unite risolvono l'enigma: l'utilizzabilità del "captatore informatico" nel processo penale*, cit., p. 3570.

[38] In questo senso R. ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezze di una recente riforma*, cit., p. 544".

[39] Cfr. Cap. II.

[40] Il comma 2 *bis* dell'art. 89 disp. att. c.p.p. impone l'utilizzo di programmi conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia e prescrive che le comunicazioni intercettate siano trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica. La previsione è stata parzialmente attuata dal D.M. 20 aprile 2018 recante "*Disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'art. 7 commi 1 e 3 del decreto legislativo 29 dicembre 2017, n. 216*", il cui art. 4 reca alcune previsioni piuttosto generiche in merito alle caratteristiche che i programmi devono avere. In particolare, la norma stabilisce che essi sono elaborati "in modo da assicurare integrità, sicurezza e autenticità dei dati captati su tutti i canali di trasmissione riferibili al captatore" (comma 1). I sistemi di sicurezza consentono che solo gli operatori autorizzati abbiano accesso agli strumenti di comando e funzionamento del captatore (comma 2). I medesimi sistemi di sicurezza prevedono a) misure di offuscamento o evasione per impedire l'identificazione del captatore e degli atti captati sia da parte di operatori umani, che per mezzo di specifico *software*; b) misure idonee ad assicurare la permanenza e l'efficacia del captatore sul dispositivo durante tutto il periodo di attività autorizzata e con i limiti previsti dal provvedimento autorizzativo, in modo da garantire il completo controllo da remoto (comma 3). Ancora, i programmi informatici devono consentire la trasmissione di tutte le informazioni necessarie a definire il contesto dell'acquisizione (comma 4). Infine, essi sono periodicamente adeguati a *standard* di funzionalità ed operatività in linea con l'evoluzione tecnologica (comma 5).

[41] Sul tema, R. BRIGHI, *Funzionamento e potenzialità invasive del* malware, in AA.VV., *Nuove norme in tema di intercettazioni,* cit., p. 221; P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, cit., p. 235 ss.; F. CASSIBBA, *La circolazione delle intercettazioni tra "archivio riservato" e "captatore informatico",* in AA. VV., *Le nuove intercettazioni*, cit., p. 101 ss.; C. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo,* cit., p. 1218; P.P. RIVELLO, *Le intercettazioni mediante captatore informatico*, cit., p. 101 ss.; S. SIGNORATO,

Tuttavia, come spesso accade, la prassi non è conforme a quanto teorizzato dal legislatore, determinando uno "scollamento" tra la realtà investigativa e le norme chiamate a regolarla. E, infatti, proprio come accade in fase procedimentale, l'impiego del captatore informatico non sembra affatto limitato alla sola captazione di conversazioni e comunicazioni tra presenti ma esteso al complesso di attività che il *Trojan Horse,* almeno in potenza, agilmente effettua e che, *de facto*, rientra nella più generale disciplina dei controlli preventivi.

4. IL *VIRUS* DI STATO QUALE TECNICA DI SORVEGLIANZA DI MASSA

Sempre nell'ambito delle investigazioni proattive, il captatore informatico è largamente impiegato per condurre sorveglianza di massa quale strumento privilegiato di acquisizione di dati e informazioni su reati o attività criminali, «al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti» [42].

Più nel dettaglio, i Servizi di *intelligence* governativa, in ragione dell'espletamento delle proprie funzioni di informazione e sicurezza, procedono alla raccolta massiva di dati e informazioni avvalendosi del captatore informatico e delle sue infinite funzioni.

Attività di investigazione "passiva", potrebbe essere definita, in cui non esistono elementi di natura oggettiva (indizianti) e soggettiva (individualizzazione del monitorato) che giustificano l'attività di prevenzione, né sussiste la necessità di alcuna autorizzazione da parte dell'autorità giudiziaria[43]: l'obiettivo, in questa fase, è solo quello di raccogliere dati e conservarli, per poi eventualmente operare uno *screening* degli stessi a scopi di prevenzione "in senso stretto", ossia di neutralizzazione di un pericolo individuato.

In questo contesto, allorquando viene percepito il pericolo concreto di una minaccia da contenere, i dati appresi in via informatizzata vengono "elaborati" attraverso appositi programmi di analisi che, sulla base dell'applicazione di "criterio di rischio" (c.d. *target*) non predeterminabili ma individuati sulla scorta dell'emergenza contingente, consentono di ricavare inferenze statisticamente rilevanti per fini di "*foreign intelligence*", ossia procedere all'individuazione di persone che fino a quel momento non sono sospettate di essere coinvolte in gravi reati.

L'esito positivo dell'incrocio informatizzato dei dati è indicativo di un "sospetto", da avvalorare attraverso successive verifiche non automatizzate. In particolare, mediante un processo di *Forensic Intelligence Analysis*[44] – che consente una visione olistica di tutte le

---

Modalità procedimentali dell'intercettazione tramite captatore informatico, cit., p. 235.

[42] È la definizione di «operazione di *intelligence* criminale» contenuta nell'art. 2, comma 1, lett. *c*, del d.lgs. n. 54 del 2015, attuativo della decisione quadro 2006/960/GAI.

[43] L'individuazione da parte della polizia giudiziaria dell'utenza telefonica da sottoporre ad intercettazione attraverso il monitoraggio di utenze presenti in una determinata zona, mediante apparecchiature in grado di individuarne i codici identificativi previo posizionamento in prossimità del cellulare da "tracciare", rientra tra gli atti urgenti e "innominati" demandati agli organi di polizia giudiziaria, ai sensi degli artt. 55 e 348 c.p.p.non soggetto ad una preventiva autorizzazione dell'autorità giudiziaria. (In motivazione la Corte ha precisato che la mera attività di individuazione dell'identità del singolo apparecchio telefonico mediante il monitoraggio di una utenza, non operando alcuna intrusione nelle conversazioni in transito sull'apparecchio monitorato e costituendo unicamente il presupposto operativo di una successiva attività captativa di conversazioni, non necessita di un decreto autorizzativo, in quanto non lesiva di alcun principio costituzionale e sovranazionale e non assimilabile ad un mezzo di ricerca della prova). Cass., sez. IV, 12 giugno 2018, n. 41385, in *C.E.D. Cass.,* n. 273929.

[44] La *Forensic Intelligence Analysis* può essere intesa come un processo di *data mining* che dall'insieme dei dati inferisce la visione ricostruttiva dei fatti. Quest'analisi ha lo scopo di leggere in

informazioni raccolte – gli uomini di *intelligence* si servono delle tipiche attività di spionaggio mirate[45] in modo da trasformare quei sospetti vaghi e non individualizzati in elementi investigativi atti a giustificare la richiesta di intercettazioni e controlli preventivi sulle comunicazioni. Così, una volta raccolti gli «elementi investigativi che giustificano l'attività di prevenzione», i Servizi di *intelligence* procedono all'esecuzione delle "tipiche" investigazioni proattive (di cui all'art. 226 disp. att. c.p.p., richiamato dall'art. 12, l. 133/12), al fine di raccogliere indizi idonei ad avviare la pre–inchiesta volta alla ricerca della *notitia criminis*[46], la cui iscrizione determina il formale inizio delle indagini preliminari condotte attraverso l'espletamento delle più o meno tradizionali investigazioni "giudiziarie".

Di qui, l'arco procedimentale", segnato dall'iscrizione della notizia di reato nell'apposito registro e culminante con l'emanazione della sentenza, sembra essersi arricchito di una fase pregiudiziale assai ampia in cui si saldano le analisi in tempo reale compiute in fase preventiva (c.d. attività di acquisizione informativa) e l'ulteriore trattamento effettuato dalle autorità di *law enforcement* (c.d. investigazione proattiva). La conseguenza inevitabile è che le intercettazioni e i controlli preventivi sulle comunicazioni, prodromiche all'acquisizione di informazioni "per" la formazione della *notitia criminis*[47], diventano l'immediata conseguenza dell'attività informatizzata di procacciamento dei dati acquisiti su larga scala che vengono "trattati" ed individualizzati allorquando viene percepito un pericolo concreto.

---

maniera assolutamente congiunta ed interdisciplinare tutti gli indizi per fornire un quadro globale nel quale le tracce si rafforzano mutuamente. «Solo in questo modo, tutte le notizie provenienti dalle investigazioni perdono il loro singolo significato (che da solo potrebbe essere fuorviante o inutile) ed arrivano ad incastrarsi tra loro come tessere di un unico mosaico che nasconde il disegno criminoso che l'investigatore è chiamato a decriptare». Così L. ROCKWELL–L. SARAVO, *L'analisi logica delle tracce,* in AA. VV., *Manuale delle investigazioni sulla scena del crimine*, a cura di D. Curtotti–L. Saravo, Giappichelli, 2019, p. 382 s.

[45] Tra queste, in base alla tipologia di fonte informativa, si possono distinguere: attività di *Osint* (*Open Source intelligence*, ossia raccolta delle informazioni mediante l'analisi di fonti aperte); di *Imint* (*Imagery intelligence*, ossia raccolta delle informazioni mediante l'analisi di fotografie aeree o satellitari); di *Humint* (*Human intelligence*, ossia raccolta delle informazioni mediante contatti interpersonali); di *Sigint* (*Signal intelligence*, ossia raccolta delle informazioni mediante l'intercettazione e analisi di segnali, sia tra persone sia tra macchine); *Techint* (*Technical intelligence*, riguardante armi ed equipaggiamenti militari); *Masint* (*Measurement and Signature intelligence*, ossia raccolta delle informazioni non classificabili nelle precedenti categorie). Una simile distinzione è rintracciabile in . CONTI–M. TORRE, *Spionaggio digitale nell'ambito dei* social network, cit., p. 535 ss. Più in generale, M. DI STEFANO, Intelligence *e* privacy *nelle macroaree: un approccio COMINT/OSINT*, in *Altalex quotidiano di informazione giuridica*, 12 dicembre 2014.

[46] È ampiamente riconosciuta la possibilità di svolgere inchieste preparatorie finalizzate alla formazione della notizia di reato, che possono trarre spunto da «qualsiasi motivo di sospetto, non importa se ricavato da un documento anonimo, da un incrocio di dati, da un'indagine statistica o se altrimenti partorito da una fertile fantasia investigativa». Così R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis*?,* in *Riv. it. dir. proc. pen.,* 1996, p. 587.

[47] Come noto, l'intercettazione preventiva di per sé non può essere considerata come notizia di reato, infatti, quest'ultima dovrà essere reperita in via autonoma attraverso una diversa fonte di informazione. Tuttavia, nulla esclude che le informazioni ottenute a seguito dell'esecuzione delle operazioni di cui all'art. 226 disp. att. c.p.p. possano rappresentare la base della c.d. pre–inchiesta, volta a ricercare un ulteriore dato da cui far dipendere l'inizio del procedimento penale. Così, i dati acquisiti in fase preventiva costituiscono solo uno spunto investigativo utile a stimolare la p.g. a svolgere indagini dirette alla ricerca della notizia di reato con le modalità e nelle forme del codice di rito. Sul tema, si consenta un rinvio a W. NOCERINO, *Le intercettazioni e i controlli preventivi. Riflessi sul procedimento probatorio*, cit., p. 184 ss.

Questo c.d. "ciclo investigativo d'*intelligence*", ossia il complesso di passaggi che permettono l'acquisizione degli elementi investigativi sui quali si fonda la richiesta di intercettazioni preventive[48], ha inizio con operazioni di «*intelligence* criminale»[49], collocandosi in una «fase procedurale precedente all'indagine penale, nella quale un'autorità competente incaricata dell'applicazione della legge, ai sensi della legislazione nazionale, ha facoltà di raccogliere, elaborare e analizzare informazioni su reati o attività criminali, al fine di stabilire se sono stati commessi o possono essere commessi in futuro atti criminali concreti» [50].

In sostanza, attraverso la sorveglianza di massa si procede al controllo *ex ante* di gruppi di soggetti non identificati ma individuati sulla scorta dei criteri elaborati attraverso l'uso proattivo dei dati, funzionali, almeno in tesi, a svelare sospetti criminali o terroristi ancora ignoti [51].

4.1. *SEGUE*: UN'INEDITA FORMA DI CAPTAZIONE E CONTROLLO PREVENTIVO: L'*IMSI CATCHER*

Meno conosciuto rispetto al captatore informatico ma altrettanto usato dagli "addetti ai lavori", è l'*IMSI Chatcher*[52], un dispositivo elettronico attraverso cui le Forze di polizia[53] e i Servizi di *intelligence* possono monitorare tutti i dispositivi elettronici presenti in un certo raggio di azione, identificare i titolari delle utenze individuate e procedere alla captazione di comunicazioni e al tracciamento dei dati che transitano sulla macchina bersaglio.

La dottrina tende ad inquadrare l'attività condotta dagli investigatori a mezzo di *Catcher* nell'ambito delle intercettazioni preventive, con ciò prevedendo un decreto motivato dell'autorità giudiziaria che autorizzi il compimento delle operazioni e ne individui i limiti applicativi[54].

---

[48] La richiesta di intercettazioni preventive è subordinata alla presenza di elementi investigativi atti a giustificare l'attività di prevenzione che, *de facto*, derivano da un'attività preventiva atipica di *intelligence* o di polizia.

[49] Così P. TROISI, Passenger Name Records, privacy *e accertamento penale*, in *Proc. pen. giust*., 2019, f. 1, p. 176.

[50] È la definizione di «operazione di *intelligence* criminale» contenuta nell'art. 2, comma 1, lett. *c*, del d.lgs. n. 54 del 2015, attuativo della decisione quadro 2006/960/GAI.

[51] G. TIBERI, *La direttiva UE sull'uso dei dati del codice di prenotazione (PNR) nella lotta al terrorismo e ai reati gravi*, in *Quaderni cost.*, 2016, p. 592.

[52] L'*IMSI Chatcher* (c.d. "Cacciatore di *IMSI*) è un "falso" ripetitore che si interpone tra il telefono "bersaglio" e le torri delle compagnie telefoniche ("*man in the middle"*), in modo da agganciare tutti i cellulari presenti nel suo raggio di azione. Sui profili tecnici, L. CAMPORESI, *Introduzione alle intercettazioni telefoniche, ambientali ed informatiche*, in *www.mobileprivacy.it.* Sui profili giuridici, A. CAMON, *Il cacciatore di IMSI,* in *Arch. pen*., 2020, f. 1, p. 1 ss.

[53] Nel luglio del 2013 la Direzione centrale della polizia criminale del dipartimento di pubblica sicurezza avvia la procedura di gara per l'acquisto di un "Sistema *IMSI Catcher* per il monitoraggio e la localizzazione di terminali radiomobili in tecnologia *2G/3G/LTE–4G*" da destinare al servizio polizia scientifica della Direzione Centrale Anticrimine della polizia di Stato. L'oggetto della fornitura è un "sistema integrato", "chiavi in mano", "trasportabile, impiegabile ed alimentabile con autoveicoli commerciali", per monitorare e localizzare i terminali radiomobili. Nel febbraio 2014 viene venduto al Ministero dell'Interno il sistema *IMSI Catcher* a un costo di circa 385 mila. A seguito di un'ulteriore gara d'appalto, nel 2015 vengono acquistati, per circa 700 mila euro, di altri due integrati per funzionalità IMSI *catcher*, ovvero per il "monitoraggio e localizzazione dei terminali radiomobili attraverso l'impiego di un unico *kit* trasportabile, impiegabile ed alimentabile con autoveicoli commerciali".

[54] In questo senso M. DI STEFANO–B. FIAMMELLA, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (Profili di* intelligence), cit., p. 167 s. *Contra* la giurisprudenza di legittimità, per cui «[L]l'individuazione da parte della polizia giudiziaria dell'utenza telefonica da sottoporre

Tuttavia, la scelta di attribuire allo strumento *de qua* la funzione di una tradizionale microspia, volta, cioè, alla mera captazione e alla registrazione delle conversazioni e delle comunicazioni in entrata e in uscita, appare eccessivamente semplicistica: l'uso sempre più frequente del *Catcher*, soprattutto durante le indagini preventive d'*intelligence*, impone una più attenta riflessione in ordine all'inquadramento sistematico della relativa attività investigativa, al fine di individuare il regime giuridico a cui le captazioni in esame devono soggiacere.

Ogni considerazione di tipo giuridico deve inevitabilmente prendere le mosse dall'analisi del dato tecnico, ossia dalla conoscenza (seppur superficiale) dello strumento con il quale le indagini vengono condotte; ciò perché i nuovi ritrovati della tecnica e delle scienze non offrono solo nuove modalità di esecuzione di "vecchi istituti processuali" ma, spesso, rappresentano attività inedite, "casi" e "modi" originali, che mal si conciliano con le categorie probatorie esistenti e richiedono un'attenta analisi dello studioso, degli operatori del diritto e della giurisprudenza, sulla loro compatibilità con le libertà costituzionali che tendono ad invadere.

In particolare, lo strumento è in grado di monitorare tutte le utenze localizzate in un preciso raggio di azione e, attraverso l'estrapolazione dell'*IMSI* (*International Mobile Subscriber identity Module*)[55], individuare il soggetto fisico cui la SIM risulta intestata. Una volta determinato il cellulare–obiettivo, il *Catcher*, disattivando l'uso dell'algoritmo di cifratura a *standard* GSM A5, riesce a comunicare con l'antenna in chiaro e, conseguentemente, a registrare le conversazioni che avvengono tramite il dispositivo monitorato[56].

L'identificazione dei soggetti e la captazione delle conversazioni che gli stessi intrattengono mediante il cellulare non sono le uniche attività che lo strumento consente di svolgere. Infatti, il *Catcher* riesce anche ad identificare – oltre il codice IMSI – anche l'IMEI[57], intercettando un bersaglio in movimento con la presenza di un ponte virtuale in grado di captare il segnale GSM, così da fungere da geo–localizzatore. Non solo. Con l'impiego di ulteriori strumenti che implementano le potenzialità del *Catcher* (c.d. *Decifer*), gli investigatori possono svolgere contemporaneamente sul dispositivo individuato ed identificato, attività di intercettazione e controllo da remoto attraverso l'inoculazione del captatore informatico, finendo così per "gestire" la macchina "infettata" e controllare ogni spostamento e attività che il soggetto compie.

Proprio in ragione delle infinte potenzialità del *Catcher*, il giurista è chiamato a verificare la conformità dello strumento di indagine alla disciplina delle intercettazioni ovvero se l'attività *de*

---

ad intercettazione attraverso il monitoraggio di utenze presenti in una determinata zona, mediante apparecchiature in grado di individuarne i codici identificativi previo posizionamento in prossimità del cellulare da "tracciare", rientra tra gli atti urgenti e "innominati" demandati agli organi di polizia giudiziaria, ai sensi degli artt. 55 e 348 c.p.p., non soggetto ad una preventiva autorizzazione dell'autorità giudiziaria». Cass., sez. IV, 12 giugno 2018, n. 41385, in *C.E.D. Cass.*, n. 273929.

[55] L'*IMSI* è il numero seriale che identifica la scheda telefonica SIM di un utente a cui è abbinato un numero di telefono.

[56] In sostanza, il *Catcher* può forzare i dispositivi al *downgrade* del *network* di connessione da 3G/4G a GSM. In tal modo permette anche l'uso di sistemi di intercettazione attiva con modalità di tipo *man–in–the–middle* (MITM). Possiede anche la capacità di fungere da disturbatore di cellulari e abbattere il segnale in ambienti circoscritti che necessitano di un alto livello di protezione (quali prigioni, ambasciate, sale per summit, aule di tribunale) che si trovano all'interno del raggio di azione (c.d. "disturbatore *Jammer*"). Come sostenuto dalla giurisprudenza di legittimità, «[…] deve ritenersi che le intercettazioni dei colloqui con i detenuti e gli internati è consentita, a pena di inutilizzabilità, solo se autorizzata debitamente nelle forme di legge». Così Cass., sez. I, 30 aprile 1992, n. 1905, in *C.E.D. Cass.*, n. 190395. Nello stesso senso, sez. VI, 29 maggio 2001, 29679, in *Cass. pen.* 2002, f. 12, p. 3152 ss.

[57] L'IMEI è il numero seriale che identifica l'apparato cellulare di trasmissione, ossia il terminale telefonico a tecnologia GSM. Cfr. M. DI STEFANO–B. FIAMMELLA, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (Profili di* intelligence), cit., p. 42

qua debba più correttamente rientrare nella categoria delle investigazioni atipiche preventive "per" la formazione del *quantum* indiziario che consenta al p.m. di autorizzare l'esecuzione delle intercettazioni e i controlli preventivi sulle comunicazioni di cui all'art. 226 disp. att. c.p.p.

Come anticipato, appare assai discutibile la scelta di ricomprenderlo nel *genus* delle intercettazioni preventive che hanno solo ad oggetto conversazioni e comunicazioni (telefoniche, ambientali o informatiche), devono essere dirette verso un soggetto noto e ben individuato e devono essere eseguite nel rispetto dei limiti di tempo e luogo indicati nel decreto autorizzativo.

Intanto, l'*IMSI Catcher* è in grado di cumulare le caratteristiche tecniche dei più tradizionali strumenti investigativi, non limitandosi alla sola captazione di conversazioni e comunicazioni transitanti sui dispositivi elettronici "infettati". Proprio come già rilevato in relazione alla "versione originaria" del captatore informatico[58], non può trattarsi di una nuova modalità attraverso cui espletare un vecchio istituto processuale, ma di una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un *quid pluris* alle ordinarie potenzialità dell'intercettazione, attuando una sorta di "controllo *online*", per cui ogni atto del soggetto monitorato viene captato.

In secondo luogo, l'apparecchio riesce ad individuare tutti gli spostamenti del controllato, dando luogo ad un'attività che, come dimostrano orientamenti dottrinali e giurisprudenziali ormai consolidati, non è assimilabile alle intercettazioni di conversazioni e comunicazioni, rientrando *tout court* nei "pedinamenti"[59], ossia nell'ambito delle investigazioni atipiche che possono essere condotte dagli investigatori in fase preventiva per raccogliere i dati utili alle determinazioni del p.m., ovvero alla formazione della *notitia criminis*[60].

Oltre criticità di ordine sistemico, determinate dall'ampiezza delle facoltà del *Catcher,* la scelta di inquadrare l'attività *de qua* nell'ambito delle intercettazioni determina conseguenze rilevanti sotto il profilo giuridico, traducendosi nella necessità di essere espletate solo dopo l'emissione di un decreto autorizzativo da parte dell'autorità giudiziaria che ne individui i soggetti, le utenze, ovvero l'ambiente da sottoporre a controllo. Secondo orientamenti giurisprudenziali ormai consolidati, «[…] il contenuto dell'autorizzazione deve identificare chiaramente la specifica persona da sottoporre a sorveglianza»[61]. Inoltre, l'autorizzazione a condurre intercettazioni telefoniche è subordinata alla preventiva conoscenza di una specifica apparecchiatura o di un particolare sistema da sottoporre ad intercettazione, in modo tale che per ciascuna operazione i dati di identificazione dell'apparecchio da sottoporre a verifica e controllo

---

[58] Cfr. Cass., sez. un., 28 aprile 2016, n. 26889, in *Cass. pen*., f. 12, p. 3566 ss.

[59] Cfr. Cass., sez. V, 7 maggio 2004, n. 24715, in *Cass. pen*. 2005, f. 10, p. 3036 ss. In senso conforme, sez. I, 7 gennaio 2010, n. 9416, in *C.E.D. Cass.*, n. 246774; sez. I, 13 marzo 2013, n. 24219, *ivi,* n. 255973; sez. III, 27 febbraio 2015, n. 32699, ivi, n. 264519; sez. VI, 27 marzo 2018, n. 20247, *ivi,* n. 273273.

[60] Sul punto, *ex multis*, C. FANUELE, *La ricostruzione del fatto nelle investigazioni penali*, Cedam, 2012, p. 12 ss.

[61] Così Corte EDU, sez. IV, 18 maggio 2010, *Kennedy c. Regno Unito*, n. 26839/05; Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, n. 47143/15. Si veda, inoltre, Corte EDU, sez. I, 23 febbraio 2016, *Capriotti c. Italia,* 28819/12. In quella circostanza, la Corte EDU ha affermato che la regolamentazione delle intercettazioni è compatibile con la preminenza del diritto necessaria in una società democratica solo se garantisce una protezione adeguata contro il pericolo di arbìtri lesivi della riservatezza, dovendo disciplinare, in tale prospettiva, in modo sufficientemente preciso, le categorie di persone assoggettabili al mezzo di ricerca della prova, la natura dei reati che vi possano dare luogo, l'indipendenza dell'organo deputato ad autorizzare lo strumento investigativo e le precauzioni da osservare per garantire la *privacy* degli interlocutori che siano casualmente attinti dalle captazioni senza aver alcun collegamento con l'oggetto delle indagini in corso.

devono essere precisati nel decreto autorizzativo[62]. Per le intercettazioni ambientali – che, per la «loro intrinseca natura», non necessitano dell'individuazione degli apparecchi ma si riferiscono, più genericamente, ad "ambienti" in cui deve intervenire la captazione[63] – risulterebbe assolutamente necessario che il decreto indicasse "specificamente" le situazioni ambientali (e non il luogo) oggetto di intercettazione[64].

Nessuna di tali regole è rispettata nell'ipotesi in questione, dal momento che il decreto autorizzativo non potrebbe indicare né il soggetto nei cui confronti è diretta l'attività di intercettazione, né l'utenza da controllare, risultando fino ad allora sconosciuta e, tantomeno, l'"ambiente" oggetto di captazione. Attraverso l*'IMSI Catcher*, infatti, non si monitora l'utenza di un soggetto già identificato, dal momento che lo scopo è ricercarla ed identificare l'intestatario e, solo dopo l'individuazione, si procede alla captazione delle conversazioni e la loro registrazione che può avvenire in ambienti non precisamente definiti.

Dunque, per le ragioni su esposte, deve ritenersi che l'attività *de qua* non possa essere ricompresa nell'ambito delle intercettazioni ma, per converso, debba essere inquadrata nel *genus* delle attività preventive "atipiche" finalizzate al procacciamento di dati e informazioni "per" le determinazioni del p.m.

In sostanza, gli investigatori si servono del *Catcher* al fine di procacciarsi informazioni in relazione a gruppi di individui "attenzionati", di modo da individuare i sospetti e acquisire gli elementi investigativi sui quale fondare la richiesta di intercettazioni e controlli preventivi. Così, svolgendo attività di natura atipica – svincolata da regole positivizzate – si riescono a raggiungere risultati investigativi assai più incisivi rispetto a quelli ottenibili mediante le investigazioni tradizionali, senza limiti autorizzativi e controlli giurisdizionali, violando la regola per cui risulterebbe vietato espletare, sulla base di meri sospetti[65], atti che, comprimendo i diritti

---

[62] Cfr. Cass., sez. I, 30 giugno 1999, n. 4561, in *C.E.D. Cass*., n. 214036. Come sostenuto, l'intercettazione può essere disposta sul numero di utenza fissa o mobile e/o sull'apparato telefonico utilizzato, mediante il numero di IMEI. Cfr. Cass., sez. I, 13 gennaio 2009, n. 7455, in *Giust. pen.,* 2010, f. III, p. 18, secondo cui «ai fini della validità del provvedimento che autorizza l'intercettazione è sufficiente l'indicazione nel provvedimento della sola numerazione IMEI, sempre che emerga dagli atti che l'apparecchio in tal modo individuato sia in possesso del soggetto da sottoporre ad intercettazione». Inoltre la Corte precisa che «[S]si considera legittima l'autorizzazione alla captazione delle comunicazioni svolte per mezzo di apparecchio cellulare identificato solo con il numero IMEI, atteso che tale codice rappresenta un elemento identificativo certo dell'apparecchio da sottoporre a controllo, per cui l'intercettazione può proseguire senza dover essere nuovamente autorizzata anche se l'apparecchio venga utilizzato con più schede telefoniche aventi numeri di utenza diversi, sempre che sia evidente agli atti la concreta riconducibilità dell'apparecchio all'uso normale da parte della persona da sottoporre ad intercettazione». Così Cass., sez. II, 21 marzo 2005, in *C.E.D. Cass.*, n. 231221. Sul punto, v. anche sez. IV, 28 marzo 2001, n. 17832, *ivi*, n. 218766.

[63] Sulla legittimità dei risultati intercettivi nel caso di variazione dei luoghi, si consenta un rinvio a Cap. III, § ?, nt.?.

[64] Possiamo, a questo punto, indicare due punti fermi: da una parte, il decreto autorizzativo delle intercettazioni di comunicazioni tra presenti deve contenere la specifica indicazione dell'ambiente nel quale la captazione deve avvenire solo quando si tratta di luoghi di privata dimora, con la limitazione che, in detti luoghi, tale intercettazioni possono essere effettuate «soltanto se vi è fondato motivo di ritenere che in essi si stia svolgendo l'attività criminosa»; dall'altra, per le intercettazioni di comunicazioni tra presenti da espletare in luoghi diversi da quelli indicati dall'art. 614 c.p. deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti ove questa viene condotta. Corte EDU, Grande Camera, 4 dicembre 2015, *Zakharov c. Russia*, cit. Si veda, inoltre, Corte EDU, sez. I, 23 febbraio 2016, *Capriotti c. Italia,* cit.

[65] Per una panoramica dei divieti, *ex multis*, D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 136 ss. Più di recente, si consenta il rinvio a W. NOCERINO, *Le denunce anonime come strumento di indagine. Un difficile equilibrio tra efficienza e garanzie*, in *Dir. pen. proc*., 2017, f. 12, p. 1221 ss.

fondamentali, presuppongono l'avvenuto accertamento della commissione di un fatto di reato, ovvero la presenza di "un minimo *fumus commissi delicti*"[66].

Pur se il nostro ordinamento consente agli inquirenti di condurre attività atipiche preventive, «il conoscere giudiziale non è senza limiti»[67], dovendo comunque agire nel rispetto del principio di legalità[68]: le libertà negative possono, infatti, essere incise solo nei casi previsti dalla legge; legge che, in tale circostanza, non esiste affatto. D'altra parte, l'irrinunciabilità di tali strumenti è evidente: pur comprimendo diritti fondamentali, i risultati ottenibili tramite il loro impiego sono assai efficaci nella prevenzione delle più gravi forme delittuose, per cui non è prospettabile che il sistema ne rimanga privo.

Al fine di trovare un contemperamento tra le due opposte esigenze è opportuno che lo Stato agisca nella consapevolezza che la compressione dei diritti fondamentali possa essere ammessa solo se posta in essere in un quadro imperativamente determinato dal legislatore: non potendo lasciare alla disponibilità degli inquirenti la scelta di utilizzare "nuovi" ed invasivi strumenti d'indagine[69], l'auspicio è quello di una specifica ed organica regolamentazione dell'utilizzo di nuovi strumenti investigativi, di «formidabile invadenza» non solo attraverso interventi "microchirurgici" sul codice di rito vigente, ma soprattutto tramite l'introduzione di norme *ad hoc*, che ne individuino i limiti e le modalità di impiego, nonché i confini di utilizzabilità anche nella fase prodromica all'inizio del procedimento penale.

5. LE NOTIZIE PRE–PROCEDIMENTALI COME "STIMOLO" INVESTIGATIVO: LE INFORMAZIONI *ANTE DELICTUM* SERVENTI LA *NOTITIA CRIMINIS.*

L'inoculazione del captatore informatico su un dispositivo elettronico portatile di un soggetto – non indagato ma –"attenzionato" dalle Forze di polizia o dai Servizi d'*intelligence* consente agli investigatori di acquisire una quantità di dati assai più cospicua rispetto a quella che si realizzerebbe attraverso l'impiego delle tradizionali microspie, avendo, in questo caso, il vantaggio che la captazione non risulta nè legata ad un ambiente specifico da monitorare né alla "mera" apprensione di conversazioni e comunicazioni, conferendo all'attività in esame maggiore flessibilità ed efficacia.

Di qui, il rischio che le informazioni acquisite possano trovare una forma di impiego – seppur in maniera indiretta – nel processo penale.

Da un punto di vista formale, può dirsi che il legislatore, nella riformulazione definitiva dell'istituto delle intercettazioni preventive[70], abbia inteso garantire l'asetticità del procedimento penale, depurato da qualunque contaminazione "esterna" al fine di contenere il pericolo di "manipolazioni investigative" da parte degli organi inquirenti.

---

[66] In questo senso A. MARANDOLA, *I registri del pubblico ministero. Tra notizia di reato ed effetti procedimentali,* Cedam, 2001, p. 113.

[67] Così M. NOBILI, *La nuova procedura penale,* Il Mulino, 1989, p. 113; ID., Il *"diritto delle prove" ed un rinnovato concetto di prova,* in *Legislaz. pen.,* 1989, p. 395 ss.

[68] Cfr. C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, Cedam, 2007, p. 158.

[69] Ciò almeno per tre ragioni: in primo luogo si rischierebbe un ricorso abusivo a tali strumenti; in secondo luogo perché si potrebbero verificare incoerenze e contraddizioni rispetto ad altri atti soggetti ad una disciplina codicistica assai rigorosa; infine perché si potrebbero creare contrasti giurisprudenziali che implicherebbero automaticamente disparità di trattamento tra i soggetti monitorati. Così C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 248 ss.

[70] Per commenti sulla complessa vicenda legislativa, L. FILIPPI, *Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali*, in *Dir. pen. e proc.,* 2002, f. 1, p. 163 ss.; S. QUATTROCOLO, *Disposizioni urgenti in contrasto al terrorismo internazionale*, in *Legislaz. pen*., 2002, f. 1, p. 70 ss.

In particolare, l'estraneità al terreno processuale delle intercettazioni preventive è corroborata dalla «*exclusionary rule*»[71] di cui al comma 5 dell'art. 226 disp. att. c.p.p., ai sensi del quale gli elementi acquisiti attraverso le attività preventive non possono essere «in ogni caso […] utilizzati nel corso del procedimento penale, fatti salvi i fini investigativi». La regola di esclusione probatoria dei risultati delle captazioni e dei controlli preventivi sulle comunicazioni è, poi, rafforzata dal divieto di pubblicizzazione delle informazioni apprese, a mente del quale «in ogni caso […] le notizie […] non possono essere menzionate in atti di indagine né costituire oggetto di deposizione né essere altrimenti divulgate»[72].

Più nel dettaglio, «[…] lo sbarramento a qualsivoglia utilizzo nel procedimento penale dei risultati delle captazioni e dei controlli preventivi sulle comunicazioni è […] funzionale ad impedire che, nell'intera area procedimentale, vengano veicolate notizie acquisite in base a criteri che obbediscono prevalentemente a scelte discrezionali del potere esecutivo»[73].

A prescindere dalle riserve sollevate in merito all'incompatibilità tra la regola di esclusione probatoria e la verifica dei presupposti applicativi delle intercettazioni preventive, la dottrina rileva che la «ridondante e insicura»[74] formulazione del disposto dia adito a non pochi dubbi interpretativi, determinando un *vulnus* difficilmente sanabile.

In particolare, la clausola di salvaguardia – che consente l'impiego dei dati appresi per sole finalità investigative[75] – desta perplessità in ordine al complesso coordinamento con il divieto probatorio precedentemente menzionato.

Posto che la locuzione *de qua* debba intendersi riferita all'attività di prevenzione in senso stretto e non essere estesa anche alla successiva fase delle indagini preliminari, ci si interroga sulla sorte delle informazioni apprese prima del formale inizio del procedimento penale allorquando attraverso l'esecuzione delle intercettazioni e dei controlli *ante delictum*, pur correttamente attuati per finalità preventive, si scopra l'avvenuta consumazione del reato per cui le operazioni di neutralizzazione sono state autorizzate.

---

[71] La definisce così E. ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma*, in *Arch. n. proc. pen*., 2016, f. 6, p. 575.

[72] Come sostenuto da E. ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma,* cit., p. 575, «[…] lo sbarramento a qualsivoglia utilizzo nel procedimento penale dei risultati delle captazioni e dei controlli preventivi sulle comunicazioni è […] funzionale ad impedire che, nell'intera area procedimentale, vengano veicolate notizie acquisite in base a criteri che obbediscono prevalentemente a scelte discrezionali del potere esecutivo». Nello stesso senso, B. AGOSTINI, *La disciplina delle intercettazioni preventive nel sistema antiterrorismo*, cit., p. 156; D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmos*i *inevitabile, ancora orfana di regole*, in *Proc. pen. giust.,* 2018, f. 3, p. 438. Come evidenzia F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, in AA. VV., *Il processo penale tra politiche della sicurezza e nuovi garantism*i, a cura di G. Di Chiara, Giappichelli, 2002, p. 25, «[…] [la] raccomandazione [è] diretta ad impedire che i risultati delle investigazioni preventive possano condizionare i giudici […] nel senso che avrebbe dovuto essere cancellata dal fascicolo processuale ogni traccia delle notizie acquisite mediante le intercettazioni preventive».

[73] Si esprime così E. ANDOLINA, *Le intercettazioni e i controlli preventivi,* cit., p. 575.

[74] Così la definisce F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 22. Sull'infelice formulazione del disposto anche G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, cit., p. 1460.

[75] Inserita in sede di conversione del decreto, «perché in caso contrario le intercettazioni preventive sarebbero state del tutto inutili, non potendosi, sulla base delle stesse, avviare le necessarie investigazioni. […] Tuttavia, si è ritenuto di tutelare la corretta formazione della prova, oltre che la *privacy*, vietando che le notizie acquisite, a seguito di intercettazioni preventive, vengano a conoscenza del giudice del dibattimento». Così Relazione dell'on. Pecorella, in *Atti Camera*, XIV leg., Assemblea, seduta del 19 novembre 2001, Resoconto stenografico, p. 16.

La situazione non è dissimile da quanto accade in tema di perquisizioni preventive[76] e di misure di prevenzione[77]. Tali attività, perennemente in bilico tra profilassi e repressione[78], al pari

[76] Le perquisizioni preventive, da collocarsi nell'ambito dell'attività di prevenzione, sono finalizzate ad evitare la commissione di determinati reati. Non vanno, quindi, confuse con le perquisizioni di polizia giudiziaria (artt. 247 ss. c.p.p.) che, per contro, si basano su una notizia di reato già acquisita. Si tratta di attività esperibili in presenza di meri indizi di reità, in relazione a peculiari contesti e scenari criminosi ritenuti talmente pericolosi ed allarmanti da giustificare l'intervento immediato della polizia giudiziaria (ufficiali ed agenti) senza alcun prodromico intervento dell'autorità giudiziaria: la stessa, tuttavia, sarà tenuta ad un controllo *ex post*, dovendo convalidare l'atto al fine di conferirgli validità processuale. Le tipologie di "intervento speciale" sono numerose e contenute in leggi promulgate *ante* o *post* codice vigente: in tema di violazione di leggi finanziarie, l'art. 33, l. 7 gennaio 1929, n. 4 consente perquisizioni domiciliari quando sussiste il sospetto di un reato; in tema di possesso di armi, esplosivi e strumenti di effrazione, da una parte l'art. 4, l. 22 maggio 1975, n. 152, autorizza gli ufficiali e gli agenti di polizia, a eseguire perquisizioni sul posto o sulla persona il cui atteggiamento o la cui presenza non appare giustificabile; dall'altra l'art. 19, l. 26 marzo 2001, n. 128, consente anche ai militari delle Forze armate di effettuare perquisizioni sul posto qualora siano in corso operazioni di sorveglianza e controllo di obiettivi fissi, al fine di accertare il possesso di armi, ovvero impedire comportamenti pericolosi per l'incolumità delle persone o per la sicurezza delle strutture; in tema di delitti di criminalità organizzata, l'art. 27, comma 2 della l. 19 marzo 1990, n. 55, regola le perquisizioni sia personali che locali durante le operazioni di polizia per la prevenzione dei reati di criminalità; in tema di produzione e traffico di sostanze stupefacenti, ai sensi degli artt. 103 e 99 d.P.R. 9 ottobre 1990, n. 309, la perquisizione locale o personale è consentita durante il corso di un'operazione per la prevenzione, al fine di rinvenire sostanze stupefacenti o psicotrope; in tema di contrasto all'immigrazione clandestina, secondo l'art. 12, comma 7, d.lgs. 25 luglio 1998, n. 286, qualora sia in corso un'operazione strumentale al contrasto, possono eseguirsi perquisizioni locali, comprese quelle domiciliari, se sussiste il fondato motivo di ritenere che i mezzi di trasporto o cose trasportate possano essere impiegati per la commissione di reati collegati al favoreggiamento dell'immigrazione clandestina. Sono, inoltre, previste perquisizioni preventive speciali: dalle norme sull'ordinamento penitenziario (artt. 34 e 35, l. 26 luglio 1975, n. 354; art. 74 d.P.R. 30 giugno 200, n. 230); in tema di illeciti amministrativi (art. 13, l. 24 novembre 1981, n. 689); in tema di produzione e commercio di sostanze alimentari, bevande, sostanze a uso agrario o prodotti agrari (l. 30 aprile 1962, n. 283 e l. 30 dicembre 1959, n. 1234). In tutti questi casi, l'atto investigativo preventivo rappresenta «l'occasione della "presa d'iniziativa" di una notizia di reato; [..] acquisita la notizia di reato, la polizia giudiziaria dovrà immediatamente trasmettere l'informativa al p.m.». Così R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, Jovene, 2010, p. 42. Sulle perquisizioni "speciali" durante la vigenza del Codice del 1930, P. BALDUCCI, voce *Perquisizioni (dir. proc. pen.),* in *Enc. dir*., XXXIII, Giuffrè, 1983, p. 137 ss.; S. ERCOLI, voce *Perquisizioni ed ispezioni*, in *Noviss. dig. it.,* V, Utet, 1984, p. 860 ss.; U. PIOLETTI, voce *Perquisizioni,* in *Noviss. dig,. it*., XXII, Utet, 1965, p. 1001 ss.; G. RICCIO, *Le perquisizioni nel codice di procedura penale*, Jovene, 1974, p. 76 ss.; A. SCAGLIONE, *Le perquisizioni nel codice di procedura penale e nelle leggi speciali*, Cedam, 1987, p. 99 ss. Per una panoramica delle perquisizioni speciali *post* 1988, G.M. BACCARI, *Perquisizioni alla ricerca della notizia di reato: il problema della validità del conseguente sequestro,* in *Cass. pen*., 1996, f. 2, p. 893 ss.; M. BARGIS, voce *Perquisizione*, in *Dig. pen*., IX, Utet, 1995, p. 498 ss.; F. TAGLIENTE, *Le attività di iniziativa della polizia giudiziaria nel nuovo processo penale*, in *Riv. polizia,* 1989, p. 729 ss. Più di recente, G. BELLANTONI, sub *artt. 247–252,* in *Codice di procedura penale commentato*, V ed., cit., p. 2427 ss.; A. CISTERNA, *Perquisizioni in caso di fondato motivo*, in *Guida dir.,* 2008, f. 16, p. 66 ss.; L. D'AMBROSIO–P.L. VIGNA, *La pratica di polizia giudiziaria*, Cedam, 2007, p. 318 ss.; P. FELICIONI, *Ispezioni e perquisizioni*, Giuffrè, 2004, p. 307 ss.; M. MONTAGNA, *La ricerca della prova nelle investigazioni di polizia giudiziaria e nelle indagini Preliminari (ispezione, perquisizione e sequestro),* in AA. VV., *La prova penale*, cit., p. 96 ss.; A. MORGIGNI, *L'attività della polizia giudiziaria*, Giuffrè, 2002; P.P. PAULESU, *Perquisizioni sul posto*, in AA. VV., *Contrasto al terrorismo interno ed internazionale*, a cura di R. Kostoris–R. Orlandi, Giappichelli, 2006, p. 284 ss.; N. TRIGGIANI, *Ispezioni, perquisizioni e sequestri*, in AA. VV., *Le prove*, a cura di A. Scalfati, in *Trattato di Procedura penale*, diretto da G. Spangher, Utet, 2009, p. 386 ss.

[77] Le misure di prevenzione «sono disposte *ante* o *praeter delictum*, nei confronti di soggetti […]

delle intercettazioni e dei controlli preventivi sulle comunicazioni, possono rappresentare forme di conoscenza di un evento criminoso.

La *quaestio* concerne la possibilità di attribuire agli elementi acquisiti attraverso le operazioni di ascolto e controllo la qualifica di *notitia criminis*[79], ovvero escludere una simile opzione ermeneutica mancando i presupposti necessari per trasformare un mero "fatto" in notizia di reato

sospettati (sulla base di elementi di fatto) di essere dediti a traffici delittuosi pericolosi per la società». Le definisce in tal modo, T. PADOVANI, *Diritto penale*, Giuffrè, 1993, p. 439. Circa la possibilità di scoprire la *notitia criminis* nel corso del procedimento di prevenzione, va rilevato che nel corso della attività investigative preventive deputate alla ricerca dei presupposti legittimanti tali misure, può accadere che si venga a conoscenza dell'avvenuta consumazione del fatto di reato, ovvero emergere una notizia ulteriore rispetto a quella oggetto del procedimento in corso o concluso. In questi casi, alcune norme autorizzano espressamente il compimento di atti di indagine: basti pensare all'art. 2 *bis* della l. 31 maggio 1965, n. 575, recante "*Disposizioni contro la mafia*", come sostituito *ex* art. 1, l. 19 marzo 1990, n. 55, ai sensi del quale: «[I]il procuratore della Repubblica o il questore territorialmente competente a richiedere l'applicazione di una misura di prevenzione procedono, anche a mezzo della guardia di finanza o della polizia giudiziaria, ad indagini sul tenore di vita, sulle disponibilità finanziarie e sul patrimonio dei soggetti […] nei cui confronti possa essere proposta la misura di prevenzione della sorveglianza speciale della pubblica sicurezza con o senza divieto od obbligo di soggiorno, nonché, avvalendosi della guardia di finanza o della polizia giudiziaria, ad indagini sull'attività economica facente capo agli stessi soggetti, allo scopo anche di individuare le fonti di reddito. […] Le indagini sono effettuate anche nei confronti del coniuge, dei figli […] nonché nei confronti delle persone fisiche o giuridiche, società, consorzi od associazioni, del cui patrimonio i soggetti medesimi risultano poter disporre in tutto o in parte, direttamente o indirettamente […]. Il procuratore della Repubblica e il questore possono richiedere, direttamente o a mezzo di ufficiali o agenti di polizia giudiziaria, ad ogni ufficio della pubblica amministrazione, ad ogni ente creditizio nonché alle imprese, società ed enti di ogni tipo informazioni e copia della documentazione ritenuta utile ai fini delle indagini nei confronti dei soggetti di cui ai commi precedenti. Previa autorizzazione del procuratore della Repubblica o del giudice procedente, gli ufficiali di polizia giudiziaria possono procedere al sequestro della documentazione con le modalità di cui agli articoli 253, 254 e 255 del codice di procedura penale»; ovvero, ai sensi del successivo comma 2 *ter*, «[N]nel corso del procedimento per l'applicazione di una delle misure di prevenzione previste dall'articolo 3 della legge 27 dicembre 1956, n. 1423, iniziato nei confronti delle persone indicate nell'articolo 1, il tribunale, ove necessario, può procedere ad ulteriori indagini oltre quelle già compiute a norma dell'articolo precedente». Da tali attività può emergere una notizia di reato che deve essere trasmessa, tramite informativa, al pubblico ministero, ovvero può essere acquisita direttamente da quest'ultimo qualora l'inchiesta preventiva sia stata condotta personalmente dallo stesso.

[78] In questo senso A. BALSAMO, *Le modifiche in materia di misure di prevenzione e di espulsione degli stranieri,* in AA. VV., *Il nuovo pacchetto antiterrorismo*, a cura di R.E. Kostoris–F. Viganò, Giappichelli, 2015, p. 40.

[79] La notizia di reato «è un concetto "polisenso", poiché indicativo sia del "contenitore", cioè il veicolo informativo, sia del "contenuto", ossia il fatto storico rappresentato». Cfr. R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, cit., p. 10; A. ZAPPULLA, *La formazione della notizia di reato*, Giappichelli, 2012, p. 120. Essa consiste «nell'informazione ricevuta dal pubblico ministero o dalla polizia giudiziaria di un fatto costituente reato, direttamente o indirettamente, per dichiarazioni di terzi o per immediata percezione». Così G. BELLAVISTA–G. TRANCHINA, *Lezioni di diritto processuale penale*, Giuffrè, 1987, p. 57. Nello stesso senso, G. ARICÒ, voce *Notizia di reato*, in *Enc. dir*., XXVII, Giuffrè, 1979, p. 760. Conferma l'assunto, G. FUMU, sub art. *333 c.p.p*., in *Commento al nuovo codice di procedura penale*, coordinato da M. Chiavario, Utet, 1990, p. 54 s.

qualificata[80], idonea a legittimare – una volta avvenuta l'iscrizione nell'apposito registro – l'avvio dell'*iter* procedimentale[81].

Da un'accurata disamina del disposto di cui al comma 5 dell'art. 226 disp. att. c.p.p., si evince che il divieto di menzione, di deposizione e di divulgazione non risulta limitato alle sole «notizie» acquisite nel corso del pre–procedimento ma estende i suoi effetti anche alle «attività di intercettazione preventiva di cui ai commi precedenti»[82]. Di qui, come rilevato, «l'eventuale notizia di reato appresa nel corso di tali attività rimarrebbe avvolta nel mistero per quanto riguarda i tempi e i modi della sua acquisizione con evidente pregiudizio per la linearità e la trasparenza della fase germinale dell'inchiesta»[83].

---

[80] La notizia di reato si compone di due elementi: la percezione di un dato e la sua qualificazione come penalmente rilevante, ovvero come corrispondente ad una fattispecie incriminatrice. Più in particolare, la notizia di reato deve contenere una proporzione referenziale corrispondente almeno agli elementi del reato che rappresentano la materialità dello stesso. In tema, A. MARANDOLA, *I registri del pubblico ministero tra notizia di reato ed effetti procedimentali,* cit., p. 58; D. NEGRI, Fumus commissi delicti. *La prova per le fattispecie cautelari*, Giappichelli, 2004, p. 77. Ma già G.M. BACCARI, *Perquisizioni alla ricerca della notizia di reato: il problema della validità del conseguente sequestro*, in *Cass. pen.,* 1996, f. 2, p. 895 ss.; L. CARLI, *La* "notitia criminis" *e la sua iscrizione nel registro di cui all'art. 335 c.p.p.*, in *Dir. pen. proc.,* 1995, f. 2, p. 736 s.; P.L. VIGNA, *Polizia giudiziaria e pubblico ministero nelle indagini preliminari: acquisizione della* notitia criminis e *ricerca delle fonti di prova*, in *Gius. pen*., 1990, f. II, p. 394 ss. In giurisprudenza, Cass., sez. V, 13 marzo 1992, n. 899, in *Cass. pen*., 1993, p. 393 ss.; sez. I, 6 novembre 1992, n. 4575, in *C.E.D. Cass*., n. 193161.

[81] Sul punto, diffusamente, F. GIUNCHEDI, Le *attività di prevenzione e di ricerca di* intelligence, in AA. VV., *La prova penale,* cit., p. 1 ss. Per onestà intellettuale va detto che in epoca più recente – pur in assenza di pronunce sul tema – si sta assistendo ad un graduale superamento della *quaestio de qua* e alla tendenza ad adottare soluzioni meno rigose e rispettose degli *standard* normativi ma sicuramente improntante alla conservazione delle informazioni utili per il raggiungimento della verità processuale. Si pensi, ad esempio, alla riconosciuta possibilità di qualificare come notizie di reato anche informazioni viziate da inutilizzabilità perché ottenuto dalle dichiarazioni della persona sottoposta alle indagini in assenza dell'avvertimento di cui all'art. 64, comma 3, lett. *c)* c.p.p (Cass., sez. V, 30 settembre 2016, n. 45016, non massimata) ovvero la possibilità di fondare la richiesta di intercettazioni "giudiziarie" sulla base dei dati emersi dalle captazioni disposte ai fini di controllo dei soggetti sottoposti a misure di prevenzione antimafia, *ex* art. 78 del Codice Antimafia. Cfr. Cass., sez. II, 19 gennaio 2016, n. 4777, in *C.E.D. Cass*., n. 266234, secondo cui «[I]in tema di intercettazione di conversazioni o comunicazioni, la richiesta di autorizzazione può legittimamente fondarsi sui risultati dell'attività captativa eseguita *ex* art. 78 d.lgs. 6 settembre 2011, n. 159 (Codice antimafia), in quanto i limiti di utilizzabilità previsti dal comma terzo del predetto art. 78 (secondo cui gli elementi acquisiti possono essere utilizzati solo per la prosecuzione delle indagini e sono privi di ogni valore a fini processuali) escludono che le conversazioni captate possano assumere valore di prova o di indizio cautelare, ma non anche che tali conversazioni possano essere poste a fondamento di un successivo provvedimento di autorizzazione all'esecuzione di intercettazioni telefoniche o ambientali, essendo quest'ultima una attività correlata alla specifica fase della prosecuzione delle indagini, che non assume diretto valore processuale».

[82] Va, invece, chiarito, che il divieto di menzione non comprende i dati esterni delle comunicazioni: il diverso ambito operativo delle due attività rischia di favorire l'ingresso di tali notizie nel patrimonio di conoscenza dell'organo giudicante, «pur essendo incorporate in documenti e atti di cui il p.m. deve disporre l'immediata distruzione». Rileva tale incongruenza, F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 27. Nello stesso senso, R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, cit., p. 64, nt. 117.

[83] Si esprime così F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 25. Nello stesso senso, anche, L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 9. Sul punto anche R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, cit., p. 64, nonché A. JANNONE, *Operazioni* under cover *contro i legami con la droga*, in *Guida dir*., 2001, f. 50, p. 37.

Inoltre, le notizie apprese in sede di intercettazioni e controlli preventivi non detengono i contenuti minimi richiesti per poter integrare gli estremi di una *notitia criminis*, mancando «la concretezza e la specificità»[84]; caratteristiche, queste, che consentono di attribuire materialità all'informazione ricevuta, distinguendola da mere congetture o illazioni e, più in generale, da ogni elemento cognitivo vago e indeterminato[85].

In effetti, in sede di attività preventiva può emergere qualche dato che evochi la possibilità di configurare un reato (indizio o sospetto) ma al fine di saggiare la consistenza di tale deduzione è doveroso svolgere accertamenti ricorrendo alle attività investigativa processuale.

In sostanza, i dati ottenuti tramite intercettazioni e controlli preventivi rappresentano "sospetti" o "indizi" di reato, cioè fatti dai quali è possibile dedurre, per lo più attraverso massime di comune esperienza, l'esistenza di ulteriori fatti, ma «solo questi [ultimi] possono essere riferiti al frammento nucleare del reato e non già i primi»[86].

Di conseguenza, l'informazione di cui si abbia la disponibilità in fase preventiva non può costituire una *notitia criminis* dal momento che «il sospetto è un elemento che agisce prima e fuori dal processo»[87], servendo esclusivamente ad indirizzare le indagini pre–procedimentali.

Posto che l'intercettazione preventiva di per sé non può essere considerata come notizia di reato e che quest'ultima dovrà essere reperita in via autonoma attraverso una diversa fonte di informazione, nulla esclude che l'atto possa rappresentare la base della c.d. pre–inchiesta, volta a ricercare un ulteriore dato da cui far dipendere l'inizio del procedimento penale. Così, i dati acquisiti in fase preventiva costituiscono solo uno spunto investigativo utile a stimolare la p.g. a svolgere indagini dirette alla ricerca della notizia di reato con le modalità e nelle forme del codice di rito[88].

---

[84] Così R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 8 ss. Oltre alla "specificità" e alla "concretezza" integrano i connotati salienti della *notitia criminis* anche l'"ipoteticità" (e, dunque, richiede la verifica della sua fondatezza mediante le indagini preliminari in vista dell'esercizio dell'azione penale) e la "riconoscibilità" della fonte. In questo senso P.P. PAULESU, voce *Notizia di reato*, in *Dig. pen*., Agg. VI, Utet, 2011, p. 358 s. Per contro, in passato, la dottrina riteneva che per la notizia di reato non è richiesto nessun requisito di forma. Così G. FOSCHINI, *Scritti anonimi e scienza privata del giudice*, in *Riv. it. dir. pen*., 1951, f. 1, p. 175 ss. Nello stesso senso G. LEONE, *Trattato di diritto processuale penale*, f. III, *Le impugnazioni*. *Processo di prevenzione criminale. Esecuzione,* Jovene, 1961. Conformemente la giurisprudenza. Cfr. Cass., sez. I, 10 marzo 1992, n. 1117, in *Arch. nuova proc*. pen., 1992, f. 2, p. 777 ss.; sez. I, 13 ottobre 1986, n. 14337, in *C.E.D. Cass*., n. 174677; sez. I, 12 dicembre 1983, n. 2179, in *Cass. pen*., 1985, f. 2, p. 725 ss.; sez. I, 10 luglio 1973, n. 1387, in *Cass. pen*., 1975, f. 1, p. 304 ss.

[85] Sul tema, *amplius*, A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 143 ss.

[86] Cfr. R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 17.

[87] Così G. ARICÒ, voce *Notizia di reato*, cit., p. 759. Nello stesso senso anche A. MARANDOLA, *I registri del pubblico ministero,* cit., p. 51.

[88] Propendono per una simile soluzione, B. AGOSTINI, *La disciplina delle intercettazioni preventive nel sistema antiterrorismo*, cit., p. 156; E. ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma*, cit., p. 576; R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, cit., p. 65; R. CANTONE–L. A. D'ANGELO, *Una nuova ipotesi di intercettazione preventiva,* cit., p. 81 s.; F. CAPRIOLI, *Le disposizioni in materia di intercettazioni e perquisizioni*, cit., p. 25; L. D'AMBROSIO, *La pratica di polizia giudiziaria,* cit., p. 418 ss.; L. FILIPPI, *Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali*, cit., p. 169; L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 9; G. GARUTI, *Le intercettazioni preventive nella lotta al terrorismo internazionale*, cit., p. 271; G.G. MEZIO, sub *art. 226 disp. att. c.p.p*., cit., p. 1069; T. RAFARACI, *Intercettazioni e acquisizione di tabulati telefonici*, in AA. VV., *Contrasto al terrorismo interno ed internazionale*, cit., p. 271; F. RUGGIERI, *D.l. 18 ottobre 2001, n. 374, convertito con modificazioni in l. 15 dicembre 2001, n. 438 – Disposizioni urgenti per contrastare il terrorismo internazionale. Commento all'art. 5 (Intercettazioni preventive),* cit., p. 795; S. SIGNORATO, *Le*

In definitiva, la disposizione esplicita ciò che si ritiene debba avvenire in relazione alle altre fonti spurie "per" la formazione della notizia di reato[89], in tema di delazioni anonime[90] o provenienti dai confidenti (informatori) della polizia giudiziaria[91], di colloqui investigativi

indagini digitali. Profili strutturali di una metamorfosi investigativa, cit., p. 320; A. VELE, *Le intercettazioni nel sistema processuale penale. Tra garanzie e prospettive di riforma*, Cedam, 2011, p. 46. Ma già R. DINACCI, *Commento all'art. 266 c.p.p.,* in *Codice di procedura penale ipertestuale,* a cura di A. GAITO, Utet, 2001, p. 3096; G. FUMU, sub *art. 226 disp. att. c.p.p.,* cit., p. 151.

[89] Trattasi di altri tipi di informazioni irrituali che determinano un'inversione del paradigma normalmente assunto per l'espletamento delle indagini «ove l'investigazione si diparte dalla *notitia criminis* quale unico elemento attinto "dal mondo dei fatti" per l'intervenuto mutamento naturalistico della realtà" e legittimano la pre–inchiesta del pubblico ministero o della polizia giudiziaria al fine di attribuire credibilità e veridicità ai dati ottenuti». Così A. MARANDOLA, *I registri del pubblico ministero,* cit., p. 91. In tema, anche R. APRATI*, La notizia di reato nella dinamica del procedimento penale*, cit., p. 45; G. COLAIACOVO, *I limiti di operatività delle denunce anonime*, cit., 4327. Si precisa, tuttavia, che in queste ultime ipotesi l'assunzione, benché informale, di una notizia di reato non avviene «menomando un diritto costituzionalmente garantito». Così L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 9.

[90] Sono anonime le denunce a cui manca la sottoscrizione o la stessa risulta imperfetta, oltre a quelle carenti di una qualsiasi indicazione che consente di rilevare obiettivamente l'identità dell'autore. La denuncia, dunque, è anonima quando «non è attribuibile ad alcuno». Così F. CORDERO, *Procedura penale*, Giuffrè, 2012, p. 752. Nello stesso senso, *ex multis*, R. CANTONE, *Denunce anonime e poteri investigativi del pubblico ministero*, in *Cass. pen*., 1996, f. 10, p. 2982 ss.; M. MERCONE, *L'inutilizzabilità penalprocedimentale degli anonimi*, in *Cass. pen*., 1995, f. 2, 750 s.; U. PIOLETTI, *Il concetto di "scritto anonimo" è diverso o più vasto di quello di "non scritto"*, in *Riv. pen.*, 1935, p. 1218 s. Nello stesso senso anche la giurisprudenza. Cfr. Cass., sez. I, 25 gennaio 1979, n. 2208, in *Cass. pen.*, 1980, f. 5, p. 1096 ss. Se il sistema previgente, prevedendo una fase istruttoria diretta all'acquisizione delle prove anteriormente al dibattimento, ammetteva l'utilizzo delle denunce anonime come "spunto conoscitivo per lo svolgimento dell'attività pre–istruttoria", l'attuale sistema accusatorio, sostituendo l'istruzione con una fase investigativa orientata all'esercizio dell'azione penale, prevede l'uso delle denunce anonime perché diventino "*input* per l'attività investigativa ai fini dell'acquisizione della notizia di reato". In tema, R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 1 ss.; G. DEAN, *Delazioni anonime e condizionamento dell'azione penale*, in *Giur. it.,* f. II, 1989, p. 257 ss.

[91] Il canale preferenziale di approvvigionamento di dati assai rilevanti per la formazione della *notitia criminis*, è la "voce" dei confidenti (gli informatori) della polizia giudiziaria. Poiché il legislatore non ha fornito alcuna definizione all'informatore di p.g., la giurisprudenza ha provveduto a colmare tale lacuna: «[...] gli informatori della polizia giudiziaria da individuarsi nei "confidenti" che, agendo di regola dietro compenso in denaro o in vista di altri vantaggi, forniscono alla polizia giudiziaria [...] notizie da loro apprese». Così Cass., sez. II, 7 novembre 2007, n. 46023, in *C.E.D. Cass.*, n. 239265. Il potere–dovere d'indagine attribuito agli organi investiganti integra un antecedente necessario per l'avvio di un procedimento penale che trova fondamento negli elementi di riscontro acquisiti e trasfusi successivamente nella comunicazione alla autorità giudiziaria. Si tratta, *tout court*, di notizie provenienti da fonti "tendenzialmente" anonime, infatti, né il giudice, *ex* art. 203 c.p.p., né il pubblico ministero, *ex* art. 362 c.p.p., possono obbligare la polizia giudiziaria a rivelare il nome degli stessi. Per una disamina sui profili processuali della *quaestio*, N. TRIGGIANI, sub *art. 203 c.p.p.,* in *Codice di procedura penale commentato*, V ed., cit., p. 2076 ss. La relatività della disciplina *de qua* deriva dal fatto che la scelta dell'anonimato dipende dall'operatore di p.g., che decide se mantenerla o meno. Cfr. Cass., sez. VI, 5 luglio 2004, n. 39232, in *Giust. pen.*, 2006, f. 3, p. 137 ss., secondo cui: «[...] la facoltà di tacere la fonte delle notizie confidenziali va riconosciuta solo quando l'informazione concerna la condotta penalmente rilevante di terzi soggetti, ma non quando – come nel caso in esame – oggetto della *notitia criminis* è proprio la rivelazione stessa, idonea a configurare ipotesi di reato a carico dell'informatore. Ritenere, diversamente, significherebbe ammettere che l'ordinamento facoltizza il confidente a commettere il reato di calunnia». Vengono, di norma, trascritte nelle relazioni di servizio e, dunque, inutilizzabili sia in dibattimento che nelle altre fasi procedimentali, ai sensi dell'art. 203, comma 1 *bis* c.p.p., introdotto dall'art. 7 della l. 1 marzo 2001,

condotti dal personale di polizia giudiziaria[92] nonché dal Procuratore Nazionale Antimafia e Antiterrorismo[93] al fine di acquisire da detenuti od internati informazioni utili sui delitti di criminalità organizzata, terrorismo, anche internazionale, e di eversione all'ordinamento democratico[94] o, ancora, di notizie apprese dai Servizi di informazione e sicurezza[95].

n. 63. Tuttavia, grazie alle stesse, la polizia giudiziaria può avviare un'attività di indagine al fine di verificare la fondatezza del dato "grezzo" e trasformarlo in notizia di reato, promuovendo, così l'avvio di un rituale procedimento penale. Non rappresentando una *notitia criminis*, l'informazione confidenziale non fa sorgere l'obbligo alla polizia giudiziaria di informare il pubblico ministero: il dovere di comunicazione subentra solo alla conclusione della pre–inchiesta, quando risulta che dalla stessa siano emersi elementi tali da attribuire a tale voce una valenza processuale. Come sapientemente rilevato, pur non costituendo *notitia criminis*, possono comunque essere considerati elementi investigativi idonei, soprattutto se corroborati da notizie di contesto, a supportare un'intercettazione preventiva. In questo senso A. JANNONE, *Operazioni* undercover *contro i legami con la droga*, cit., p. 36. Come sostenuto, «[I]in tema di autorizzazione alle operazioni di intercettazione, il divieto di utilizzazione di informazioni confidenziali è espressamente limitato alla valutazione dei gravi indizi di reato e non opera qualora la fonte anonima si limiti a riferire agli inquirenti il numero dell'utenza utilizzata dall'indagato già autonomamente attinto da gravi indizi di reità per il reato oggetto del procedimento». Così Cass., sez. IV, 16 novembre 2007, n. 108, in *C.E.D. Cass.*, n. 238254.

[92] Ai sensi dell'art. 18 *bis,* l. 26 luglio 1975, n. 354, la polizia giudiziaria può procedere a colloqui investigativi al fine di acquisire informazioni utili per la prevenzione o la repressione dei delitti di criminalità organizzata, ovvero dei delitti commessi con finalità di terrorismo, anche internazionale od eversione all'ordinamento democratico.

[93] *Ex* art. 18 *bis* ord. penit., che, quale atto privilegiato del più generale potere di raccolta, di elaborazione delle conoscenze e di coordinamento generale, conferisce al Procuratore Nazionale Antimafia la facoltà di procedure a colloqui con detenuti od internati. Parte della dottrina tende a distinguere i colloqui informativi della p.g. da quelli del PNA: in quest'ultimo caso, infatti, la finalità dell'atto risulterebbe quella di incentivare il detenuto ad assumere il ruolo di collaboratore di giustizia, e, quindi, durante l'audizione verrebbero essere rilasciate dichiarazioni già costituenti *notitia criminis.* In questo senso R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., 40.

[94] Il colloquio investigativo si risolve, in sostanza, in un atto atipico informale non utilizzabile a fini processuali. Cfr. Cass., sez. V, 14 ottobre 1996, n. 873, in *C.E.D. Cass.,* n. 206904. Va, tuttavia, specificato che la scelta dell'anonimato è questa volta attribuita al dichiarante stesso: a quest'ultimo spetta il diritto di scegliere se rendere o meno le sue dichiarazioni processualmente utilizzabili; ove, infatti, il soggetto decida di rendere dichiarazioni non avvalendosi della garanzia dell'anonimato, le stesse sono configurabili come *notitia criminis.* Sul tema, *ex plurimis*, R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit. 62; G. SANTACROCE, *I colloqui investigativi,* in *Riv. polizia,* 1994, f. III–IV, p. 15 ss.; G. SALVINI, *I colloqui investigativi e i permessi di soggiorno a fini investigativi per il contrasto del terrorismo,* in AA. VV., *Le nuove norme di contrasto al terrorismo*, cit., p. 1 ss.

[95] Ai sensi dell'art. 23, comma 7 della l. 3 agosto 2007, n. 124, i Direttori dei Servizi di Informazione per la Sicurezza e il Direttore generale del D.I.S. sono tenuti a trasmettere agli organi di polizia le informazioni che possono costituire notizia di reato apprese nell'esercizio delle proprie funzioni. I dati così ottenuti potranno essere processualmente utilizzabili solo a condizione che la polizia giudiziaria ne abbia verificato la fondatezza, in quanto provenienti da attività informative che sono per lo più di carattere illecito (art. 17, l. 124/2007), ovvero svolte sotto copertura (art. 24, l. 124/2007) e, quindi, scarsamente attendibili. Si veda, M.L. DI BITONTO, *Raccolta di informazioni e attività di* intelligence, cit., p. 153 ss.; T.F. GIUPPONI, *La riforma del sistema di informazione per la sicurezza della Repubblica,* in AA. VV., *Nuovi profili del segreto di Stato e dell'attività di* intelligence, cit., p. 53 ss., ID., *Servizi di informazione e forze di polizia dopo la legge n. 124/2007,* in *Astrid Rassegna*, n. 10, 2009; R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 227 ss.

In particolare, deve essere reciso ogni riferimento alla fonte che ha dato l'avvio alla ricerca della notizia di reato e, una volta che questa sia acquisita, il legame con l'atto preventivo non deve risultare da alcun atto processuale e, conseguentemente, nemmeno dalla stessa *notitia criminis.*

Una volta attribuita alle intercettazioni preventive funzione "servente" alla formazione della notizia di reato, resta da chiedersi in che cosa si sostanzi l'attività di ricerca espletabile dagli organi inquirenti e dagli uomini dell'*intelligence* durante la pre–inchiesta e quali sono le attività che, *de facto*, possono essere eseguite per acquisire informazioni "qualificate" al cominciamento del rito penale[96].

Preliminarmente va chiarito che la possibilità di condurre una "pre–inchiesta", deputata ad appurare la concretezza e la veridicità delle informazioni irritualmente ricevute, non è riservata esclusivamente ai Servizi di informazione, indiscussi protagonisti della fase preventive, ma è concessa anche alle Forze di polizia.

Più nel dettaglio, tale facoltà è conferita, implicitamente dall'art. 330 c.p.p.[97] che, riconoscendo alla polizia giudiziaria (artt. 55 e 348, comma 3 c.p.p.)[98] il potere di prendere "notizia di reato di propria iniziativa"[99], legittima l'uso dei dati acquisiti in sede preventiva quale «presupposto euristico suscettibile di attivare investigazioni preordinate all'individuazione della *notitia criminis*»[100].

---

[96] Nella distinzione tra notizie di reato "qualificate" e "non qualificate", parte della dottrina ha sostenuto che esistesse un *tertium genus*, costituito dalle "notizie qualificate negativamente, cioè poste dalla legge *extra ordinem*, voci correnti nel pubblico, delazioni e testimonianze anonime". Così P. CORSO, *Notizie anonime e processo penale*, Cedam, 1977, p. 231. Sulla differenza tra notizie qualificate e notizie di reato non qualificate, esaustivamente, R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 23 ss.; A. MARANDOLA, *I registri del pubblico ministero,* cit., p. 62 ss.

[97] Cfr. P.P. PAULESU, sub *art. 330,* in *Codice di procedura penale commentato*, V ed., cit., p. 3001.

[98] La possibilità di condurre la pre–inchiesta è attribuita dall'art. 330 c.p.p. anche al p.m. (artt. 56 e 326 c.p.p.). Il dato, tuttavia, non è scontato. In effetti, parte della dottrina avanza riserve in merito alla possibilità del pubblico ministero di condurre investigazioni preliminari, in virtù di un'interpretazione rigorosa dell'art. 330 c.p.p. *Ex multis*, F. FALATO, *Sulla natura degli atti precedenti alla iscrizione della* notitia criminis *e sull'estensibilità del divieto previsto dall'art. 62 c.p.p.,* cit., p. 1626 ss.; M. MERCONE, *L'inutilizzabilità penalprocedimentale degli anonimi*, cit., p. 754 s.; R. ORLANDI–F. CAPRIOLI–G. INSOLERA, *La ricerca della notizia di reato da parte dell'accusatore*, in *Criminalia,* 2011, f. 1, p. 440; D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 136 s.; G. SANTALUCIA, *Il potere del pubblico ministero di ricerca delle notizie di reato tra principi costituzionali e legge processuale*, in *Riv. it. dir. proc. pen*., 2002, f. 1, p. 159 ss.; C. SCACCIANOCE, *Denunce anonime e attività "pre–procedimentali" del pubblico ministero,* in *Ind. pen*., 2006, f. 3, p. 1184 ss. Sul punto, già, P. FERRUA, *L'iniziativa del pubblico ministero nella ricerca della* notitia criminis, in *Legislaz. pen*., 1986, p. 317 ss.

[99] Ai sensi dell'art. 330 c.p.p., la notizia di reato può essere "trasmessa" ovvero "presa di iniziativa": la prima ipotesi contempla tutti i casi in cui i soggetti legittimati dalla legge presentano alla polizia giudiziaria o all'autorità giudiziaria specifici atti (denuncia, referto, querela, istanza, richiesta, informativa); la seconda, invece, le restanti modalità mediante cui una notizia entra nella sfera cognitiva degli organi inquirenti. Sul punto R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., 22.

[100] Così R. CANTONE, *Denunce anonime e poteri investigativi del pubblico ministero*, cit., p. 2988.

La dottrina[101] e la giurisprudenza[102], attraverso la predisposizione di uno «statuto della pre–inchiesta»[103], vietano il compimento di attività che presuppongono l'esercizio di poteri autoritativi[104], nel doveroso rispetto dei principi costituzionali e delle norme processuali in tema di diritto di difesa[105].

Il *discrimen* tra lecito e illecito risulta, dunque, essere rappresentato dall'uso della coercizione: in definitiva gli "investigatori" (intendendo come tali sia gli uomini dell'*intelligence* che le Forze di polizia) possono compiere «solo quegli atti che per loro natura sono incapaci di arrecare pregiudizio ai diritti degli individui»[106].

Dunque, sulla base dei dati appresi in sede di investigazione preventiva, è vietato espletare interrogatori, ispezioni, perquisizioni, sequestri ed intercettazioni[107], quali atti che, comprimendo i diritti fondamentali, presuppongono l'avvenuto accertamento della commissione di un fatto di reato, ovvero la presenza di un minimo «*fumus commissi delicti*»[108]. Se, infatti, si consentisse l'esercizio delle tipiche attività di indagine nella fase finalizzata al consolidamento della *suspicio criminis*, si rischierebbe di trasformare i mezzi di ricerca della prova in mezzi di acquisizione della notizia di reato[109].

Più nel dettaglio, si ritiene interdetta l'attività ispettiva[110] in quanto assolutamente incompatibile, *in re ipsa*, con l'assenza di una fattispecie delittuosa: se l'ispezione è volta ad

---

[101] *Ex multis* LP. FERRUA, *L'iniziativa del pubblico ministero nella ricerca della* notitia criminis, cit., p. 320 s.; U. NANNUCCI, *L'attività di iniziativa del p.m.: modelli operativi*, in *Dir. giust*., 1994, p. 938; R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, in *Riv. it. dir. proc.* pen., 1996, p. 557 nt. 29. Più di recente, R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 49 ss.; A. MARANDOLA, *I registri del pubblico ministero,* p. 51 s.; D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 138.

[102] Cass., sez. V, 28 ottobre 2008, n. 4329, in *C.E.D. Cass.,* n. 242944; sez. VI, 21 settembre 2006, n. 36003, cit.; Cass., sez. IV, 17 maggio 2005, n. 30313, cit.; Cass., sez. III, 18 giugno 1997, n. 2450, in *Arch. nuova proc. pen*., 1997, f. 5, p. 642 ss. *Contra*, sez. III, 29 aprile 2004, n. 26847, cit.; sez. III, 19 aprile 2011, n. 28909, cit.

[103] L'espressione appartiene a R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 49.

[104] Già sotto il vigente codice la dottrina aveva evidenziato l'inconciliabilità tra investigazioni conseguenti preventiva ed atti autoritativi. *Ex plurimis*, P. FERRUA, *L'iniziativa del pubblico ministero nella ricerca delle notizie di reato,* cit., p. 313 ss. Dopo l'entrata in vigore del codice vigente, G.M. BACCARI, *Perquisizioni alla ricerca della notizia di reato: il problema della validità del conseguente sequestro*, cit., p. 894 s; F. DE LEO, *Il pubblico ministero fra completezza investigativa e ricerca dei reati,* cit., p. 1449 ss.; G. FUMU, sub. *art. 333* c.p.p., cit., p. 48 ss.; A. MARANDOLA, *I registri del pubblico ministero,* cit., p. 328 s.; D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 138; A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 265. In giurisprudenza, Cass., sez. I, 17 aprile, 2012, n. 40518, in *Guida dir*., 2012, f. 27, p. 91 ss.; sez. III, 26 gennaio 1999, n. 3261, in *Cass., pen*., 1999, f. 12, p. 3458 ss.; sez. I, 28 giugno 1995, n. 2362, in *C.E.D. Cass.,* n. 201843; sez. I, 29 ottobre 1993, n. 4556, in *Cass. pen*., 1994, f. 1, p. 134 ss.

[105] Laddove, infatti, in tale fase pre–procedimentale si consentisse l'espletamento di ogni attività investigativa possibile in base al Libro V del codice di rito, si legittimerebbero «vere e proprie indagini preliminari irrituali». Così C. FANUELE, *La ricostruzione del fatto nelle investigazioni penali,* cit., p. 20.

[106] Cass., sez. III, 18 giugno 1997, n. 2450, cit., p. 642 ss.

[107] Per una panoramica dei divieti, D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 136 ss.; G. COLAIACOVO, *I limiti di operatività delle denunce anonime*, cit., p. 4326; N. ROMBI, *Anonimo, perquisizione e sequestro,* in *Cass. pen.,* 1998, f. 7, p. 2084 s.

[108] *Contra,* Cass., sez. IV, 4 giugno 1993, n. 8919, in *C.E.D. Cass.,* n. 198189.

[109] In questo senso Cass., sez. VI, 11 dicembre 1998, n. 2882, in *C.E.D. Cass.,* n. 212678.

[110] In riferimento alla preclusione delle ispezioni nella fase pre–procedimentale, compiutamente, R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 50 ss.; A. MARANDOLA, *I*

"accertare tracce o altri effetti materiali del reato", in mancanza di una concreta ipotesi di *delictum* appare assi inverosimile verificare la sussistenza degli stessi[111].

Lo stesso dovrà dirsi in relazione alle perquisizioni[112], che implicano la sussistenza di una *notitia criminis* perché si possa provvedere alla ricerca del corpo del reato o cose ad esso pertinenti[113], ed al sequestro[114], il cui requisito indispensabile per l'ammissibilità è l'astratta configurabilità dell'ipotesi delittuosa[115].

D'altra parte, come evidenziato dalla giurisprudenza[116], l'obbligo di motivazione del decreto con cui l'autorità giudiziaria dispone la perquisizione, ai sensi dell'art. 247, comma 2 c.p.p., o il sequestro, ai sensi dell'art. 253, comma 3 c.p.p., impone che nella stessa non si faccia alcun riferimento a situazioni sussumibili nell'ambito di mere congetture o sospetti[117], ma, al contrario, sia riferita alla sussistenza «di indizi di un certo rilievo»[118].

A maggior ragione non potranno essere disposte intercettazioni in virtù del "doppio vincolo" previsto dall'art. 266 c.p.p. Da una parte, infatti, per l'accesso alla captazione sono richiesti "gravi indizi di reato"; dall'altra sono previste specifiche tipologie delittuose in base alle quali è ammissibile l'intrusione nelle comunicazioni[119].

---

registri del pubblico ministero, cit., p. 115 s. Si veda, inoltre, P. MOSCARINI, voce *Ispezioni*, in *Enc. dir*., IV, Giuffrè, 1998, p. 464 s.

[111] Sul punto P.P. PAULESU, sub *art. 330,* cit., p. 3002.

[112] Per un commento, R. CANTONE, *Denunce anonime e poteri investigativi del pubblico ministero*, cit., p. 2989; F. DE LEO, *Il pubblico ministero tra completezza investigativa e ricerca dei reati,* cit., p. 1448 ss.; L. IANNONE, *Selle condizioni legittimanti la perquisizione domiciliare*, in *Cass. pen.,* 1996, f. 6, p. 1545 ss.; D. POTETTI, *Attività del p.m. diretta all'acquisizione della notizia di reato e ricerca della prova*, cit., p. 140 s.; N. ROMBI, *Anonimo, perquisizione e sequestro*, cit., p. 2084 ss. Unica eccezione al su menzionato divieto è rappresentata dalla previsione contenuta nell'art. 41 T.U.L.P.S. che, in materia di armi, munizioni o materie esplodenti autorizza le perquisizioni senza che sia formalmente iniziato il procedimento penale. Cfr. P. FELICIONI, *Le ispezioni e le perquisizioni*, cit., p. 367 ss.

[113] La ricerca del corpo del reato o dell'indagato presuppone *ab origine*, la notizia di reato. Cfr., *ex plurimis*, Cass., sez. V, 13 marzo 1992, n. 899, in *C.E.D. Cass.*, n. 190418. In dottrina, *ex multis*, T. BENE, *L'art. 191 c.p.p. e i vizi del procedimento probatorio*, in *Cass. pen.,* 1994, f. 1, p. 116 ss.

[114] In questo senso Cass., sez. V, 13 maggio 2004, n. 37941, in *C.E.D. Cass.*, n. 230174; sez. III, 29 aprile 2004, n. 26847, cit.; sez. IV, 17 maggio 2005, n. 30313, cit.

[115] Intesa come la possibile sussistenza della fattispecie delittuosa sulla base di elementi processuali già acquisiti agli atti. Cfr. Cass., sez. un., 20 novembre 1996, n. 23, in *Cass. pen*., 1997, f. 7, p. 1673 ss.

[116] Cfr. Cass., sez. VI, 27 ottobre 2007, n. 36003, in *C.E.D. Cass.,* n. 235279; sez. V, 13 maggio 2004, n. 37941, *ivi,* n. 230174.

[117] N. ROMBI, *Anonimo, perquisizione e sequestro*, cit., p. 2085.

[118] Sul *quantum* dei "concreti indizi", G. BELLANTONI, *Perquisizioni*, in *Enc. giur.,* XXIII, Treccani, 1991, p. 4 s.; F. CORDERO, *Procedura penale,* cit., p. 774; M. D'ONOFRIO, *Il sequestro preventivo,* Cedam, 1998, p. 19 s. Più di recente, G. BELLANTONI, sub *art. 247 c.p.p.,* in *Codice di procedura penale commentato,* V ed., cit., p. 2433 s.; P.P. RIVELLO, sub *art. 253* c.p.p., *ivi,* cit., p. 2459 s.

[119] Da ultimo, Cass., sez. un., 28 ottobre 2018, n. 45486, in *Proc. pen. giust*. In questa occasione, la Suprema Corte dispone l'annullamento dell'ordinanza cautelare con rinvio al Tribunale del riesame affinchè dia adeguata risposta alle obiezioni dei legali dell'imprenditore Romeo, i quali, tra l'altro, sostengono che le intercettazioni condotte attraverso l'utilizza del *virus trojan* risultano "inutilizzabili" dal momento che sono state disposte «senza una reale notizia di reato perchè Romeo non era interessato dalle indagini di criminalità organizzata che si stavano compiendo in relazione all'appalto del servizio di pulizia dell'ospedale Cardarelli». Più nel dettaglio, i giudici convegnono sul fatto che parte delle intercettazioni sono state disposte nei confronti dell'imprenditore «a prescindere dalla sussistenza di elementi indiziari nei confronti del soggetto intercettato» e che «a fronte di eccezioni puntuali della difesa, il controllo del Tribunale non risulta essere stato adeguato e la motivazione è fortemente carente».

Inoltre, l'assoluta "indispensabilità ai fini della prosecuzione delle indagini", *ex* art. 267 c.p.p., lascia presupporre che le indagini siano già state avviate sulla scorta di una *notitia criminis*[120].

Tuttavia, la scelta di precludere la transizione diretta da intercettazioni preventive a repressive o tra le prime ad un decreto autorizzativo di altri mezzi di ricerca della prova, seppur in linea con la separazione tra orizzonte preventivo e repressivo, «può determinare uno iato temporale, pragmaticamente non sempre soddisfacente, specie nelle ipotesi di gravi elementi di reità emersi sul fronte preventivo»[121].

Una volta delineati "in negativo" i poteri degli investigatori nella fase pre–procedimentale, vanno individuate le attività che, in concreto, possono essere espletate.

In base alla ricognizione fin qui effettuata, si può desumere, *a contrario*, che *ante notitia criminis* sono ammissibili tutti quegli atti "atipici" di indagine[122] che non implicano l'uso di poteri autoritativi e/o coercitivi.

Ad ogni modo, attraverso il compimento di altri atti di investigazione "per" la formazione della *notitia criminis* – sollecitati dalle informazioni apprese tramite intercettazioni e controlli preventivi – potrebbe emergere una notizia di reato "qualificata" e idonea ad istaurare il procedimento penale per l'accertamento della sua fondatezza.

Pare, allora, opportuno soffermarsi sugli obblighi postumi degli investigatori una volta appresa la notizia di reato durante l'esecuzione delle indagini proattive, distinguendo i doveri propri dei Servizi d'*intelligence* da quelle eseguibili dalla p.g.

---

[120] Risulta essere assolutamente preclusa ogni possibilità di passaggio, pur di fronte ad elementi pregnanti, da un regime di intercettazione preventiva a quello di intercettazioni giudiziarie, «giacché non è sempre agevolmente immaginabile l'intellegibilità di una situazione di flagranza assicurata da un'attività *ante delctum*, quando scollegata totalmente dal contesto in cui essa è maturata». Così A. JANNONE, *Operazioni* under cover *contro i legami con la droga*, cit., p. 37.

[121] Si esprime così S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 320.

[122] Quali, ad esempio, pedinamenti, identificazioni, rilievi segnaletici, descrittivi o fotografici, raccolta ed elaborazione di dati, schedatura di persone osservate a distanza. Sul punto v. C. FANUELE, *La ricostruzione del fatto nelle investigazioni penali,* cit., p. 21 s. Come sottolineato, in relazione alle attività preventive di polizia, deve trattarsi di atti per i quali non è prevista una «possibile partecipazione del difensore al compimento dell'atto». Così C. FANUELE, *L'utilizzazione delle denunce anonime per l'acquisizione della notizia di reato: condizioni e limiti delle attività pre–procedimentali alla luce delle regole sul "giusto processo*", cit., p. 1555.

In quest'ultima ipotesi, è noto che una volta appresa la notizia di reato, la polizia giudiziaria non è sottoposta a nessun obbligo se non a trasmetterla, senza ritardo o immediatamente[123], all'autorità giudiziaria perché provveda alla rituale iscrizione[124].

La situazione risulta alquanto diversa per i Servizi di informazione e sicurezza che, di fatto, operano senza il controllo dell'autorità giudiziaria e sono, di conseguenza, esentati dall'obbligo di riferire alla stessa le notizie di reato apprese[125].

In merito, l'art. 23 commi 6, 7 e 8, l. 123/2007, detta una peculiare disciplina che gli appartenenti ai servizi di sicurezza sono tenuti a rispettare una volta appresa la *notitia criminis* nell'esercizio delle proprie funzioni[126].

---

[123] Ai sensi dell'art. 347 c.p.p., «[A]acquisita la notizia di reato, la polizia giudiziaria, senza ritardo, riferisce al pubblico ministero, per iscritto, gli elementi essenziali del fatto e gli altri elementi sino ad allora raccolti, indicando le fonti di prova e le attività compiute, delle quali trasmette la relativa documentazione. 2. Comunica, inoltre, quando è possibile, le generalità, il domicilio e quanto altro valga alla identificazione della persona nei cui confronti vengono svolte le indagini, della persona offesa e di coloro che siano in grado di riferire su circostanze rilevanti per la ricostruzione dei fatti. 2 *bis*. Qualora siano stati compiuti atti per i quali è prevista l'assistenza del difensore della persona nei cui confronti vengono svolte le indagini, la comunicazione della notizia di reato è trasmessa al più tardi entro quarantotto ore dal compimento dell'atto, salve le disposizioni di legge che prevedono termini particolari. 3. Se si tratta di taluno dei delitti indicati nell'articolo 407 comma 2 lettera *a*, numeri da 1 a 6 e, in ogni caso, quando sussistono ragioni di urgenza, la comunicazione della notizia di reato è data immediatamente anche anche in forma orale. Alla comunicazione orale deve seguire senza ritardo quella scritta con le indicazioni e la documentazione previste dai commi 1 e 2. 4. Con la comunicazione, la polizia giudiziaria indica il giorno e l'ora in cui ha acquisito la notizia». A prescindere dall'autonomia operativa concessa alla p.g. in relazione ai tempi della trasmissione, va precisato che, qualora ricorra uno dei delitti previsti dall'art. 407, comma 3 lett. *a*, nn. da 1 a 6 e, in ogni caso, quando sussistono ragioni d'urgenza, la comunicazione va data immediatamente (*ex* art .21, l. 8 agosto 1995, n. 332). Sul punto, *ex plurimis*, L. BRESCIANI, sub *art. 347 c.p.p.*, *Commento al nuovo codice di procedura penale*, cit., p. 125 ss.; L. D'AMBROSIO–P.L. VIGNA, *La pratica di polizia giudiziaria*, cit., p. 173 ss.; G. ICHINO, *L'attività di polizia giudiziaria*, in AA. VV., *Le indagini preliminari e instaurazione del processo*, cit., p. 122 ss.; G. P. VOENA, *Investigazioni e indagini preliminari*, in *Dig. pen.,* VII, Utet, 1993, p. 33 ss. Più di recente, P. P. PAULESU, sub art. 347 *c.p.p.,* in *Codice di procedura penale commentato*, V ed., cit., p. 388 ss.

[124] Ai sensi dell'art. 335 c.p.p., una volta ricevuta la notizia, il p.m. la iscrive «immediatamente» nell'apposito registro. Per una disamina compiuta del disposto, cfr. R. APRATI, *La notizia di reato nella dinamica del procedimento penale*, cit., p. 105 ss.; ID., *Intorno all'immediatezza dell'iscrizione della notizia di reato: sindacabilità del giudice e inutilizzabilità degli atti investigativi tardivi*, in *Cass. pen*., 2005, f. 6, p. 1330 ss.; V.L. CARLI, *La* notitia criminis *e la sua iscrizione nel registro di cui all'art. 335 c.p.p.,* in *Dir. pen. proc*., 1995, f. 3, p. 736 ss.; L.D. CERQUA, *Registro delle notizie di reato*, in *Dig. pen*., III, Utet, 2005, p. 1299 ss.; A. MARANDOLA, *I registri del pubblico ministero*, cit., p. 44 ss.; A. PATANÈ, *La* notitia criminis: dall'iscrizione *formale all'iscrizione di fatto*, in *Giur. it*., 2010, p. 675 ss.; G.P. VOLPE–L. AMBROSOLI, *Registro delle notizie di reato*, in *Dig. pen.,* XII, Utet, 1997, p. 43 ss.; A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 289 ss.

[125] Escludendo che i dipendenti dei servizi d'*intelligence* possano assumere la veste di ufficiale o agente di polizia giudiziaria (art. 23 comma 1, l. 124/2007), la disposizione *de qua* indirettamente esenta tali soggetti dalla necessità di rispettare la disciplina codicistica della trasmissione della notizia di reato all'autorità giudiziaria.

[126] Sul punto, esaustivamente, E. GALLUCCI, *La nuova disciplina dei servizi* di *sicurezza, commento all'art. 23*, in *Legislaz. pen*., 2007, p. 754 ss.; G. GAMBACURTA, *I rapporti con gli altri soggetti,* in AA. VV., I *servizi di informazione e il segreto di Stato*, a cura di C. Mosca-S. Gambacurta-G. Scandone-M. Valentini, Giuffrè, 2008, p. 292 ss.; F. SOMMOVIGO, *Attività d*'intelligence *e indagine penale*, in AA. VV., *Nuovi profili del segreto di Stato e dell'attività d*'intelligence, Giappichelli, 2010, p. 247. Per una disamina della normativa previgente, per tutti, M. VALENTINI, *Profili normativi dell'attività dei servizi informativi e delle forze di polizia nel contrasto alla criminalità organizzata*, in *Riv. polizia*, 2006, p. 174 ss.

In particolare, anche il personale d'*intelligence*, oltre che i pubblici ufficiali e gli incaricati di pubblico servizio[127], è sottoposto all'obbligo di denuncia dei fatti costituenti reato[128]. Tuttavia, l'organo ricevente non è rappresentato dall'autorità giudiziaria, bensì dal Direttore dell'Agenzia o del D.I.S. di appartenenza del funzionario che apprende la notizia.

Una volta ricevuta la notizia, i Direttori sono gravati dall'obbligo di informare, senza ritardo, il Presidente del Consiglio dei Ministri e, contestualmente, di comunicare l'esistenza della *notitia criminis* ai competenti organi di polizia giudiziaria[129] che, a loro volta, sono tenuti ad attivare il tradizionale *iter* burocratico, regolamentato dal codice di rito, ovvero riferire all'autorità giudiziaria il contenuto della notizia in modo da provvedere alla consueta iscrizione[130].

5.1. *SEGUE*: I RISCHI PROCEDIMENTALI DELLE INDAGINI PROATTIVE. LA CIRCOLAZIONE DELLE INFORMAZIONI

Con l'introduzione della regola di esclusione probatoria e del divieto di menzione delle notizie apprese *ante delictum*, di cui all'art. 226, comma 5 disp. att. c.p.p., rafforzata dall'obbligo di distruzione delle informazioni ottenute di cui ai commi 3 e 3 *bis*, il legislatore ha voluto tenere fede al principio della necessaria separazione tra prevenzione e repressione e, più precisamente, degli ambiti e dei compiti di *intelligence* e di polizia al fine di evitare la circolazione degli elementi investigativi acquisiti nel corso delle indagini proattive nel processo e, conseguentemente, qualunque forma di contaminazione tra *pre* e *post* procedimento.

In sostanza, il sistema costituito tende a mantenere distinta la fase preventiva, di ricerca e analisi dei dati – propria dei Servizi di informazione per la sicurezza – da quella repressiva della giurisdizione penale, sul presupposto che le due funzioni non sono in alcun modo assimilabili[131]:

---

[127] Ai sensi dell'art. 331 c.p.p., ««[S]salvo quanto stabilito dall'articolo 347, i pubblici ufficiali e gli incaricati di un pubblico servizio che, nell'esercizio o a causa delle loro funzioni o del loro servizio, hanno notizia di un reato perseguibile di ufficio, devono farne denuncia per iscritto, anche quando non sia individuata la persona alla quale il reato è attribuito. 2. La denuncia è presentata o trasmessa senza ritardo al pubblico ministero o a un ufficiale di polizia giudiziaria. […]». Dunque obbligati a presentare denuncia sono i pubblici ufficiali e gli incaricati di un pubblico servizio, individuabili secondo le nozioni fornite dagli artt. 357 e 358 c.p. Si tratta, in particolare, di un obbligo discendente dalla peculiare qualifica ricoperta da tali soggetti, i quali risultano titolare di un dovere di collaborazione nei confronti dello Stato. Alla medesima regola, in virtù della clausola di salvezza contenuta nel comma 1, non sono sottoposti gli appartenenti alla p.g. Cfr. G. AMATO–M. D'ANDRIA, *Organizzazione e funzioni della polizia giudiziaria nel nuovo codice di procedura penale,* cit., p. 70 s.; L. D'AMBROSIO–P.L. VIGNA, *La pratica di polizia giudiziaria*, cit., p. 207.

[128] Si ritiene che ogni eventuale omissione debba essere penalmente sanzionata ai sensi dell'art. 361 c.p. In questo senso E. GALLUCCI, *La nuova disciplina dei servizi* di *sicurezza, commento all'art. 23*, cit., p. 754 s.

[129] La trasmissione della notizia agli organi di polizia giudiziaria può essere ritardata «su autorizzazione del Presidente del Consiglio dei Ministri, quando ciò sia strettamente necessario al perseguimento delle finalità istituzionali del Sistema di informazioni per la sicurezza», *ex* art. 27, comma 8, l. 124/2007.

[130] L'*iter* gerarchizzato e la previsione secondo cui il destinatario della notizia di reato proveniente dalle agenzie di informazione non è direttamente il p.m. ma la p.g. è funzionale a mantenere fede al principio di separazione tra autorità giudiziaria e servizi. In questo senso F. SOMMOVIGO, *Attività d*'intelligence *e indagine penale*, cit., p. 248 ss.

[131] Sulla necessità di tenere separati i due momenti, D. CURTOTTI, *Procedimento penale e* intelligence *in Italia*: *un'osmosi inevitabile, ancora orfana di regole,* cit., p. 442 s.; F. GIUNCHEDI, *Le attività di prevenzione*, cit., p. 3; S. SETTI, Intelligence *e indagine penale in Italia*, in *www.sicurezzanazionale.gov*, p. 2; A. SPATARO, *Politiche della sicurezza e diritti fondamentali*, in *Quest. giust*, settembre 2016, p. 210 ss. Più in generale, in relazione all'autonomia tra il

quella d'*intelligence* è tesa a ricercare ed elaborare tutte le informazioni utili a difendere la sicurezza interna ed esterna dello Stato e delle sue istituzioni democratiche da ogni minaccia, attività eversiva e forma di aggressione criminale o terroristica; quella di polizia (giudiziaria) è deputata all'accertamento dei fatti di reato[132]. Dunque, «[N]non il principio di collaborazione, ma piuttosto il principio di separatezza ha finora caratterizzato i rapporti tra queste due espressioni del potere statuale»[133].

Se questa è la condizione ideale prefigurata sul piano normativo, nella prassi si rileva tra la fase preventiva e quella processuale un rapporto osmotico e simbiotico fatto di punti di contatto e interrelazioni costanti: proprio come accade nell'ambito del processo di prevenzione[134], anche

---

procedimento di prevenzione e il procedimento penale, L. MARAFIOTI, *Sinergie tra procedimento penale e procedimento di prevenzione*, in *Dir. pen. cont.,* 22 aprile 2016.

[132] La profonda distinzione tra le funzioni di *intelligence* e di p.g. è definibile sotto un profilo di competenza. I servizi di informazione e sicurezza sono inseriti nella struttura del potere esecutivo al fine di garantire una risposta tecnica alle necessità informative del Governo mentre le autorità requirenti (quindi la polizia giudiziaria e la magistratura) sono espressione dell'autonomo potere giudiziario volto alla prevenzione ed alla repressione dei reati. Sul punto v. R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, cit., p. 583 ss.; P. TONINI, *Polizia giudiziaria e magistratura. Profili storici e sistematici,* Giuffrè, 1979, p. 245 ss.; R. VANNI, Analisi ragionata delle norme *processuali penali in tema di polizia giudiziaria*, in *Giust. pen*., 1986, f. 3, p. 449 ss.; M. VOLPI*, Costituzione e polizia*, in *Pol. dir*., 1983, p. 92 ss. Si segnala che, di recente, la *quaestio* relativa alla separazione delle competenze delle Agenzie di informazione e quelle della polizia giudiziaria è stata oggetto di attenzione della giurisprudenza europea che ne fornisce un'interpretazione teleologicamente orientata. Cfr. *Bundesverfassungsgericht*, 24 aprile 2013, n. 31 che, nel dichiarare parzialmente illegittima la legge sulla raccolta e lo scambio di dati per fini antiterrorismo, ribadisce il principio della separazione delle informazioni raccolte per fini di *intelligence* da quelle utilizzabili per fini di polizia e la necessaria tassatività dei presupposti legittimanti i poteri di acquisizione dei dati personali da parte delle Agenzie, precisando come, a fronte della estensione di tali poteri, sia ancor più necessaria un'adeguata supervisione da parte dell'Autorità di protezione dei dati. Sul punto si veda anche, Corte cost. portoghese, 28 agosto 2015, n. 124, che dichiara l'illegittimità del potere di accesso dei Servizi ai tabulati degli apparati di telefonia mobile, previsto dalla locale normazione antiterrorismo. La Corte ritiene che l'acquisizione di tali dati, in assenza di un vaglio giurisdizionale autorizzativo, analogo a quello del processo penale, costituisce un'ingerenza particolarmente grave nelle comunicazioni private.

[133] Così R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 229. Come rilevato, la separazione delle funzioni ha caratterizzato già l'esperienza nazionale durante la vigenza del codice Rocco, per cui l'attività dei servizi di sicurezza era protetta dal segreto opponibile a norma degli artt. 342 (per le prove documentali) e 352 (per le prove testimoniali) c.p.p. 1930. Nel primo scorcio di vita repubblicana, l'attività giudiziaria resta ancora separata da quella dei servizi di sicurezza: si impone l'obbligo del segreto penalmente sanzionato, derogabile solo previa autorizzazione dell'amministrazione interessata. La situazione inizia a cambiare con la legge 24 ottobre 1977, n. 801: l'art. 9 della novella, infatti, obbliga gli appartenenti ai Servizi di sicurezza a denunciare i reati dei quali fossero venuti a conoscenza nell'esercizio delle loro funzioni. Il disposto, in sostanza, introduce un'apertura del processo penale agli uomini di *intelligence*, stabilendo un canale di comunicazione tra i due corpi dello Stato che, fino a quel momento, erano concepiti come separati. Per una ricostruzione storica dei rapporti di collaborazione tra *intelligence* e p.g., R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 231 ss.; D. GROSSO, voce *Polizia giudiziaria (dir. proc. pen.),* in *Enc. giur.,* XXIII, Roma, 1990, p. 3 s.; D. NEGRI, Fumus commissi delicti. *La prova per le fattispecie cautelari*, cit., p. 84 ss.; R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, cit., p. 583 ss. Come rileva D. CURTOTTI, *Procedimento penale e* intelligence *in Italia*: *un'osmosi inevitabile, ancora orfana di regole,* cit., p. 442, «[Tra] i due settori, l'ordinamento ha sempre individuato […] momenti di contatto, ma la prospettiva iniziale è stata limitata a prevedere l'utilizzo delle "informazioni" come prova nel processo penale […]».

[134] Come noto, nell'ambito del procedimento di prevenzione, la giurisprudenza, pur avallando la

in questo ambito si riscontra un atteggiamento rivolto all'elaborazione di strategie e strumenti "ripristinatori" di elementi probatori patologicamente viziati che, tuttavia, apparirebbe esiziale espungere dal compendio probatorio a causa dell'indispensabile apporto gnoseologico che essi potrebbero fornire.

Ciò per diverse ragioni interconnesse tra loro.

In primis, il procedimento penale sembra aver mutato i suoi caratteri peculiari di asetticità e di impermeabilità rispetto a quella fase pre–procedimentale di natura prettamente investigativa. Come sostenuto, «[P]pensare ad un procedimento penale che si instaura con l'acquisizione della *notitia criminis* è immagine alquanto anacronistica e sicuramente poco aderente alla realtà»[135]. La riflessione è condivisibile. Pur non negando che tradizionalmente l'inizio dell'*iter* procedimentale è determinato dall'iscrizione della notizia di reato nell'apposito registro, non è possibile sottacere tutta l'attività preventiva e di ricerca della stessa che, inevitabilmente, indirizza le investigazioni "per" procedere alla sua formazione. A questo punto, una volta convertito il confine tra indagini proattive (compiute nella fase pre–procedimentale) e indagini preliminari, le fasi idealmente consecutive della prevenzione e della repressione «si sono agglutinate dando origine ad una lunga linea continua di tecniche operative miste, anfibie, ambivalenti»[136].

D'altra parte, la legittimazione della procura al rilascio dell'autorizzazione a procedere alle operazioni *de quibus*, contribuisce ad indebolire la pretesa impermeabilità fra il procedimento penale di prevenzione e quello di cognizione[137]. É evidente come il p.m., laddove partecipi, direttamente o indirettamente, alla ricerca preventiva della notizia di reato, «venga necessariamente introdotto negli spazi investigativi propri [della polizia di pubblica sicurezza], sì da condividerne anche le logiche improntate a scelte di opportunità ed a valutazioni ampiamente discrezionali proprie della polizia stessa»[138]. Infatti, «non sembra del tutto coerente con questa impostazione la scelta di imporre una coincidenza fra l'organo che deve autorizzare le intercettazioni preventive e l'organo che potrebbe poi instaurare un procedimento penale su fatti appresi nell'espletamento di indagini preventive; se anche il legislatore ha inteso escludere l'utilizzabilità come *notitia criminis* dei risultati captativi così ottenuti, stabilendo che essi

---

teoria dell'autonomia tra quest'ultimo e il procedimento ordinario, sembra consentire la circolazione probatoria sulla base di specifiche esigenze investigative. Cfr. Cass., sez. II, 28 maggio 2008, n. 25919, in *C.E.D. Cass.,* n. 240629; sez. I, 15 giugno 2007, n. 29688, *ivi*, n. 236670; sez. VI, 3 novembre 2005, n. 39953, *ivi*, n. 236596. In dottrina, *ex multis*, G. SILVESTRI, *La trasmigrazione e l'utilizzazione degli atti*, in AA. VV., Misure di prevenzione, a cura di S. Furfaro, Giappichelli, 2013, p. 218; C. CARINI, *Giudizio di prevenzione e intercettazioni "illegali": sui rapporti tra prevenzione e cognizione,* in *Giur. it.,* 2008, f. 2, p. 444; D. ROCCHI, *Nota sull'autonomia del giudizio di prevenzione rispetto a quello di cognizione,* in Giur. it., 2006, f. 7, p. 1483; L. MARAFIOTI, *Sinergie fra procedimento penale e procedimento di prevenzione,* in *Dir. Pen. Cont.,* 22 aprile 2014, 1 ss.; S. BELTRANI, *Intercettazioni inutilizzabili e procedimento di prevenzione: un rapporto controverso,* in *Dir. pen. proc.,* 2009, f. 1, p. 90. In questo senso, più di recente, G. PECCHIOLI, *Processo penale e procedimento di prevenzione: interferenze probarorie e limiti di utilizzabilità*, in *Dir. pen. proc*., 2020, f. 2, p. 266 ss.

[135] F. GIUNCHEDI, *Le attività di prevenzione,* cit., p. 1. Nello stesso senso, R. ORLANDI, *Inchieste preparatorie nei procedimenti di criminalità organizzata: una riedizione dell'*inquisitio generalis?, cit., p. 568 ss.

[136] L'espressione è di D. NEGRI, *La regressione della procedura penale ad arnese poliziesco* (*sia pure tecnologico),* cit., p. 47.

[137] Ai sensi del comma 1 dell'art. 226 disp. att. c.p.p., la legittimazione ad autorizzare l'esecuzione delle operazioni spetta al «procuratore della Repubblica presso il tribunale del capoluogo del distretto in cui si trova il soggetto da sottoporre a controllo ovvero, nel caso non sia determinabile, del distretto in cui sono emerse le esigenze di prevenzione […]».

[138] L'espressione appartiene a E. ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma*, cit., p. 569.

debbano essere immediatamente distrutti dopo che il procuratore della Repubblica abbia verificato l'irregolarità delle operazioni, quest'organo potrebbe sfruttare le conoscenze in ogni caso acquisite per procedere alla ricerca della notizia di reato, per dare quindi avvio al procedimento penale, e compiere specifici atti d'indagine all'esito dei quali determinarsi eventualmente per l'esercizio dell'azione penale»[139].

Inoltre, l'esperienza degli ultimi vent'anni mostra un progressivo ampliamento dei momenti di contatto tra i due asettici comparti in esame al fine di contenere le nuove emergenti esigenze investigative legate al contrasto alla criminalità organizzata di stampo mafioso ed eversivo e al terrorismo internazionale: proprio in questi settori la tangenza tra organi requirenti e Servizi di informazione per la sicurezza diviene imprescindibile e doverosamente virtuosa[140].

Se è vero che l'attività di *intelligence* è definibile come «un processo che inizia con la ricerca di informazioni della più diversa natura, prosegue con la relativa analisi e sfocia in un quadro di valutazioni volte alla comprensione e alla previsione di eventi futuri»[141], va da sé che le indagini inerenti alla criminalità organizzata e al terrorismo rappresentino il campo di naturale osmosi tra le funzioni dei Servizi di sicurezza e degli organi giudiziari e di polizia[142].

In questi settori, attività d'*intelligence* e investigativa vanno sempre più condividendo concetti strutturali e modalità operative onde condurre le indagini necessarie al perseguimento dei rispettivi obiettivi. Entrambe queste attività puntano ad acquisire informazioni su fenomeni criminosi con la caratteristica di essere spazialmente diffusi e duraturi nel tempo; entrambe agiscono prevalentemente con indagini occulte, le uniche che permettono di conoscere fenomeni delittuosi ancora in corso di svolgimento[143].

---

[139] R. ORLANDI, *Il sistema di prevenzione tra esigenze di politica criminale e principi fondamentali,* cit., p. 561.

[140] Sulle sinergie tra attività di *intelligence* e attività investigative, R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 228 s.; S. SETTI, Intelligence *e indagine penale in Italia*, cit., p. 1 s., il quale sottolinea che «[E]ntrambe queste attività basano la loro *ratio essendi* nel contrasto a quelle manifestazioni idonee a mettere in pericolo e finanche a ledere alla base l'ordinato, libero e pacifico sviluppo delle attività dei consociati. Questo contrasto non può realizzarsi più efficacemente che nella prevenzione, dunque per mezzo di accertamenti occulti, gli unici in grado di massimizzare il risultato protettivo, posto che, in alcuni casi, la risposta sanzionatoria per quanto severa non solo non riesce a porsi quale idonea controspinta, ma giunge poco utile quando ormai il risultato criminoso è stato raggiunto ed il danno è difficilmente riparabile». Anche i "tecnici" del settore aspirano all'istituzione di più concrete forme di collaborazione. Di recente, il direttore generale del DIS, ha riconosciuto come *intelligence* e magistratura perseguano «un obiettivo comune per quanto riguarda il terrorismo […] in molti campi» ma in particolar modo con l'obiettivo di estirpare il fenomeno terroristico. «Occorre», prosegue il direttore generale, «sicuramente assicurare una separatezza, ma, nel momento stesso in cui noi assicuriamo la separatezza, dobbiamo anche assicurare la cooperazione, per via delle necessità di procedere in modo integrato». Così G. MASSOLO, *Direttore generale del DIS*, nel corso dell'audizione in merito al d.d.l. 7/2015, Resoconto Stenografico della seduta n. 2 delle Commissioni II e IV della Camera dei Deputati, Roma, 4 marzo 2015, in *www.documenticamera.it.*

[141] Così G. CONSO, *Sicurezza tra informazione, segreto e garanzie*, in *Per aspera ad Veritatem*, 1995, n. 3, p. 27.

[142] Parla di «osmosi tra l'ambito della prevenzione e quello della repressione», M. GIALUZ, *Banche dati europee e procedimento penale italiano,* in AA. VV., *Cooperazione informativa e giustizia penale nell'Unione europea,* a cura di F. Peroni–M. Gialuz, EUT, 2009, p. 253.

[143] Quando si parla di "speciali tecniche investigative" si allude a modalità di indagine che hanno in comune la caratteristica di essere occulte, compiute all'insaputa della persona presa di mira, con ciò volendo ricomprendere sia l'attività tipica dei servizi di informazione e sicurezza sia quella della p.g. Cfr. Risoluzioni conclusive del convegno AIDP, Istanbul, settembre 2009, in *www.aidpitalia.org.*

L'«intrico inestricabile»[144] derivante dalla commistione funzionale tra *intelligence* e p.g. è anche favorito dalla facile fruibilità e condivisibilità degli strumenti di ultimissima generazione utilizzati nei vari ambiti di indagine[145]; strumenti nelle mani degli stessi operatori per il conseguimento di scopi differenti ma interconnessi, rispetto ai quali non è poi così facilmente possibile tracciare una netta linea di demarcazione che scinda la prevenzione dalla repressione.

Ancora, tra i fattori che hanno inciso sulla trasformazione dei rapporti tra procedimento penale e *intelligence* vi è la rimarcata esigenza di coordinamento e organicità dell'azione investigativa[146], sul presupposto che «le iniziative promosse dal potere esecutivo e iniziative giudiziarie vanno armonizzate, non condotte separatamente»[147].

[144] F. DE LEO, *Il pubblico ministero tra completezza investigativa e ricerca dei reati*, cit., p.1442,

[145] Si tratta, in particolare, di strumenti di indagine occulti a più forte carattere invasivo quali – tra gli altri – il pedinamento satellitare, sistemi di cattura elettronica dell'identità dei telefoni cellulari (c.d. *IMSI catcher*), l'ascolto dei dialoghi o la videoripresa di immagini a distanza tramite l'inoculazione di virus informatici in dispositivi elettronici di uso comune. Sul tema D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmos*i *inevitabile, ancora orfana di regole*, cit., p. 443 s.; M. DI STEFANO–B. FIAMMELLA, *Intercettazioni: remotizzazione e diritto di difesa nell'attività investigativa (Profili di* intelligence), cit., p. 167 ss.; D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* cit., p. 53; R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 235; T. RAFARACI, *Intercettazioni e acquisizione di tabulati telefonici*, in AA. VV., *Contrasto al terrorismo interno ed internazionale*, cit., p. 274; A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 252 ss.

[146] Sul tema, *amplius*, G. SCHENA, *La "debole" concentrazione distrettuale delle indagini in materia di terrorismo*, in *Dir. pen. cont.,* 2017, p. 134 ss.

[147] Si esprime così R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 229.

La «nuova cultura investigativa»[148], ispirata al principio della collaborazione reciproca, trova conferme sul piano legislativo sia interno[149] che internazionale[150], in cui viene meno «il

[148] Così la definisce D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmos*i *inevitabile, ancora orfana di regole*, cit., p. 443.

[149] Sotto il profilo interno, la l. 3 agosto 2007, n. 124, recante "*Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto*", in *Gazz. uff*., 13 agosto 2007, n. 187, segna il più significativo intervento riformatore in materia, ridisegnando i confini tra attività di *intelligence* e accertamento penale e producendo un profondo cambiamento nel modo di concepirsi, strutturarsi e operare degli organismi della giustizia penale. Più in particolare, l'art. 4 della l. 124/2007, attribuisce al Dipartimento delle informazioni per la sicurezza (DIS) – che unitamente al Presidente del Consiglio dei Ministri e al Comitato interministeriale per la sicurezza della Repubblica (CISR) compongono il sistema di informazione per la sicurezza della Repubblica – il ruolo di gestore delle «informazioni, [del]le analisi e [de]i rapporti provenienti dai Servizi di informazione per la sicurezza, dalle Forze armate e di polizia […]» e di promotore del loro coordinamento, «anche attraverso riunioni periodiche, [del]lo scambio informativo tra l'AISE, l'AISI e le Forze di polizia». Inoltre, Il rapporto collaborativo tra uomini di *intelligence* e di polizia è espressamente imposto dall'art. 12 della l. 124/2007, in forza del quale le Forze armate, quelle di polizia, gli ufficiali e gli agenti di polizia giudiziaria e di pubblica sicurezza svolgono, in relazione alle singole attribuzioni, un ruolo ancillare nel sistema investigativo preventivo, collaborando con l'AISI e con l'AISE e viceversa. V., in argomento, AA. VV., *Servizi segreti: dalla riforma dell'*intelligence *uno statuto dei rapporti con la magistratura*, in *Guida dir*., 2006, f. 33, p. 11 ss.; P. BONETTI, *Problemi costituzionali della legge di riforma dei servizi di informazione per la sicurezza della Repubblica*, in *Diritto e società*, 2008, f. 2, p. 251 ss.; R. BRICCHETTI–L. PISTORELLI, *Le forze di polizia sono tenute a collaborare, Commento a l. 3 agosto 2007, n. 124*, in *Guida dir*., 2007, f. 40, p. 57 ss.; M. CASTELLANETA, *Servizi segreti: confronto aperto sul rispetto dell'equo processo*, in *Guida al diritto comunitario e internazionale*, 2007, f. 3, p. 11 ss.; A. CORNELI, *I servizi segreti "sterzano" verso il Parlamento nella ricerca di un nuovo equilibrio tra poteri*, in *Guida dir.,* 2012, p. 11 ss.; ID., *Una visione "integrata" dell'*intelligence *per i nuovi servizi disegnati dalla riforma*, *ivi,* 2008, f. 11, p. 11 s. Sul punto, *amplius*, D. CURTOTTI, *Procedimento penale e* intelligence, cit., p. 444 s.; F. GIUNCHEDI, *Le attività di prevenzione*, cit., p. 10 ss.; S. SETTI, Intelligence *e indagine penale in Italia*, cit., p. 7. Più di recente, il d.lgs. 23 aprile 2015, n. 54, recante "*Attuazione della decisione quadro 2006/960/GAI del Consiglio del 18 dicembre 2006 relativa alla semplificazione dello scambio di informazioni e intelligence tra le Autorità degli Stati membri dell'Unione Europea incaricate dell'applicazione della legge*", si prefigge l'obiettivo di agevolare lo scambio di informazioni e di *intelligence* tra le autorità degli Stati membri dell'UE. In tema, *amplius*, G. DE AMICIS, *Scambio di informazioni e* di intelligence, in Aa. Vv., *Cooperazione giudiziaria penale*, a cura di A. Marandola, Giuffrè, 2008, p. 791 ss. Si veda, inoltre, G. MEZIO, sub *art. 226 disp. att. c.p.p*., cit., p. 1063.

[150] Nel sistema della cooperazione di polizia delineato dalla Convenzione di applicazione degli accordi di Schengen viene fissata un'articolata disciplina sullo scambio di informazioni, ispirata al principio generale secondo il quale gli Stati contraenti si impegnano a far sì che i rispettivi servizi di polizia si assistano ai fini della prevenzione e della ricerca di fatti punibili, sempre che la legislazione nazionale non riservi la relativa domanda alla competenza delle autorità giudiziarie. (art. 39, par. 1). A ciò si aggiunga il Programma dell'Aia del Consiglio europeo di Bruxelles del 4 e 5 novembre 2004, in *Gazz. Uff. CE*, C 53, 3 marzo 2005, n. 1 (cfr. AA. VV., *Cooperazione informativa e giustizia penale nell'Unione europea*, cit.; G. DI PAOLO, *La circolazione dei dati personali nello spazio giudiziario europeo dopo Prüm*, in AA. VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona*, a cura di T. Rafaraci, Giuffrè, 2011, p. 198 ss.; C. FANUELE, *Lo scambio di informazioni a livello europeo*, in AA. VV., *La circolazione investigativa nello spazio giuridico europeo: strumenti, soggetti, risultati*, a cura di L. Filippi–P. Gualtieri–P. Moscarini–A. Scalfati, Cedam, 2010, p. 19 ss.; L. SALAZAR, *Presente e futuro nello spazio di libertà, sicurezza e giustizia: dal piano d'azione dell'Aia alla 'visione' della Commissione europea*, in AA. VV., *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale*, a cura di G. Grasso–R. Sicurella, Giuffrè, 2008, p. 625 ss.; P. TROISI, *Il potenziamento della cooperazione transfrontaliera. Lo scambio di informazioni*, in AA. VV., *«Spazio europeo di giustizia» e procedimento penale italiano*, a cura di L. Kalb, Giappichelli, 2012, p. 195 ss.; ID., *La circolazione di informazioni per*

diaframma che tradizionalmente separava mondo dell'*intelligence* e sfera giurisdizionale»[151], sollecitando sinergie e punti di contatto tra i due ambiti[152].

L'assottigliarsi delle differenze tra attività di *intelligence* e procedimento penale, produce implicazioni di carattere strettamente processuale, favorendo proprio quella circolazione probatoria dei dati che il sistema originariamente aveva ripudiato.

Allo stato dell'arte, dunque, non pare peregrino il rischio di indebiti sconfinamenti funzionali e di reciproci condizionamenti che vanificano l'originario intento del legislatore di tenere separati i due comparti garantendo l'asetticità del procedimento penale[153].

Intanto, la confusione tra pre–procedimento e procedimento non solo pone in crisi gli abituali paradigmi della giustizia penale ma altera anche gli equilibri di potere, determinando un sistema ibrido, misto di profilassi e repressione, in cui gli attori della fase preventiva e di quella procedimentale si scambiano costantemente i ruoli.

In effetti, pare che nella fase pre–procedimentale anche la polizia possa muoversi «a tutto campo»[154], cominciando dall'area della pubblica sicurezza e, conseguentemente, a detenere il monopolio strategico anche della fase preventiva grazie al dominio sull'enorme mole di informazioni spurie raccolte in autonomia assai prima dell'intervento del magistrato penale[155].

---

le investigazioni penali nello spazio giuridico europeo, Padova, 2012), il Trattato di Prum del 2005 (F. GANDINI, *Il trattato di Prüm articolo per articolo. Ecco le nuove frontiere per la sicurezza. Banche dati antiterrorismo e interventi congiunti in 7 Stati Ue*, in *Dir. e giustizia*, 2006, f. 37, p. 57 ss.; A. MARANDOLA*,* Information sharing *nella prospettiva del Trattato di Prüm e della Decisione di recepimento nel quadro giuridico dell'Unione*, cit., p. 179 ss.) e la decisione 2006/960/GAI (S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in AA. VV., *Cooperazione informativa e giustizia penale nell'Unione europea*, cit., p. 88 ss.), atti a semplificare lo scambio di informazioni ed *intelligence* tra le autorità degli Stati membri incaricati all'applicazione della legge penale. Da ultimo, il regolamento 2018/1727 del 14 novembre 2018, che sostituisce e abroga la decisione 2002/187/GAI, riforma completamente, alla luce dell'art. 85 TFUE, *Eurojust* (ora Agenzia dell'Unione europea per la cooperazione giudiziaria penale), con rifermento, tra l'altro, alla competenza, alle funzioni, alla struttura, nonché allo *status* e ai poteri dei membri nazionali. Sono disciplinati, inoltre, agli aspetti operativi, il trattamento dei dati personali e i rapporti con gli altri organismi, tra cui, in particolare, la Procura europea, recentemente istituita. Per commenti, L. SALAZAR, *La riforma di* Eurojust *e i suoi riflessi sull'ordinamento italiano,* in *Dir. pen. cont.,* 2019, f. 1, p. 42 ss.

[151] Testualmente, G. MELILLO, *Il ruolo dei servizi di informazione. Il coordinamento investiga*tivo, in AA. VV., *Contrasto al terrorismo interno e internazionale*, cit., p. 230 ss.

[152] Una simile evoluzione non stupisce più di tanto lo studioso dal momento che analoghe soluzioni legislative sono riscontrabili in altri ordinamenti comparabili al nostro. Assai calzante appare il raffronto con la legge tedesca che istituisce l'autorità federale di difesa costituzionale (*Bundesverfassungsschutzbehorde*), più o meno corrispondente all'AISI. I §§ 17–20 del *Bundesverfassungsschutzgesetz* contengono previsioni assai dettagliate sulla collaborazione tra l'autorità in questione e l'autorità giudiziaria. Sul progressivo intricarsi delle due attività, F.F. MANGET, *Intelligence and the Criminal Law System,* in *Stanford Law and Policy Review*, n. 17, 2006, p. 415 ss. In realtà, il nostro ordinamento, già negli anni '70, aveva mostrato una certa apertura al principio di collaborazione tra i Servizi di intelligence e le Forze di polizia. Cfr. Corte d'Assise di Brescia, 2 febbraio 1978, in *Giur. merito*, 1979, p. 424 ss., per cui «i risultati informativi prevenienti dall'attività di *intelligence* e di p.g. possono costituire il punto di partenza per i reati commessi».

[153] Sui possibili sconfinamenti tra le due funzioni, E. ANDOLINA, *Le intercettazioni e i controlli preventivi sulle comunicazioni nel contrasto al terrorismo internazionale tra irrisolte criticità ed esigenze di riforma,* cit., p. 576; L. FILIPPI, *Terrorismo internazionale: le nuove norme interne di prevenzione e repressione. Profili processuali*, cit., p. 170; G.G. MEZIO, sub *art. 226 disp. att. c.p.p.*, cit., p. 1069.

[154] Così D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* cit., p. 47.

[155] Si assiste, in sostanza, ad un incremento delle attività riconducibili alla categoria dell'*intelligence*

Tuttavia, come noto, non esistendo un autonomo corpo di polizia per le indagini di natura repressiva[156], gli stessi uomini che svolgono le investigazioni proattive "per" la formazione della notizia di reato, si trovano a compiere anche le indagini susseguenti all'inizio del procedimento penale puro[157].

In questi casi la relazione osmotica tra *pre* e *post* procedimento, determinata da una frequente eterogenesi dei fini nell'ambito delle diverse vesti indossate contemporaneamente, appare inevitabile, dal momento che gli uomini della pre–inchiesta saranno chiamati a svolgere indagini per l'accertamento del fatto di reato con un approccio non più puro e scevro da condizionamenti esterni ma intriso delle informazioni incamerate in fase preventiva.

Non può, infine, sottacersi che è proprio la peculiare tipologia delle fattispecie di reato (terrorismo e reati associativi) coinvolte dall'attività investigativa a carattere preventivo ad accentuare il processo osmotico tra *pre* e *post delictum*. Nell'ambito di siffatti complessi contesti investigativi, infatti, la medesima attività può configurarsi come repressiva rispetto ad un reato (reato presupposto) e come preventiva rispetto ad un altro tipo di fattispecie delittuosa (reato scopo)[158], determinando la progressiva erosione della linea di confine tra le attività proprie dell'*intelligence* e quelle di polizia.

Ma la circolazione probatoria non è solo determinata dalla contiguità dell'attività di prevenzione con il contesto giudiziario ed i punti di contatto tra i due momenti, risultando

---

svolte quotidianamente dalle Forze di polizia. Sul punto M.L. DI BITONTO, *Raccolta di informazioni e attività di* intelligence, cit., 254 ss.; S. GAMBACURTA, *I rapporti con gli altri soggetti*, cit., p. 287 ss.; R. ORLANDI, *Attività di* intelligence *e diritto penale della prevenzione*, cit., p. 227 ss.; F. SOMMOVIGO, *Attività d*'intelligence *e indagine penale*, cit., p. 242 s. Il primato delle Forze di polizia anche nei settori un tempo riservati esclusivamente ai servizi d'*intelligence* trova conferma nell'art. 2, commi 2, 3 e 4 del d.l. 7/2015 in relazione alla creazione delle cc.dd. *black list* ("liste nere") dei siti internet utilizzati per l'attività di proselitismo terroristico: i fornitori dei servizi dovranno oscurare la pagina *web* segnalata dall'a.g., inibirne l'accesso e rimuovere, a seguito di una disposizione del p.m., i contenuti illeciti accessibili al pubblico potenzialmente attinenti alla finalità di propaganda terroristica. Quello che viene richiesto agli operatori di polizia, per poter disporre l'oscuramento del sito attraverso una procedura "snella e rapida" è una valutazione – discrezionale e priva di alcun controllo giurisdizionale – «sul grado di incisività e persuasività dello scritto, potenzialmente idoneo a suscitare un interesse e un certo grado di condivisione» Cfr. Cass., sez. I, 6 ottobre 2015, n. 47489, in *www.ilpenalista.it*. In questa peculiare ipotesi le indagini penali assumono la funzione servente di alimentare il flusso di dati verso l'Esecutivo grazie alle segnalazioni provenienti dalla polizia giudiziaria. Come sostenuto, «il rapporto prefigurato dalla norma tra questi ultimi e la struttura governativa adibita alla sicurezza telematica è di tipo diretto; il legislatore profitta dell'immedesimazione organica dovuta al ruolo bifronte esercitato dal personale appartenente alla Polizia postale e delle comunicazioni». Si esprime così D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* cit., p. 49. Sul tema, esaustivamente, S. SIGNORATO, *Le misure di contrasto in rete al terrorismo:* black list, *inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet,* in AA. VV., *Il nuovo pacchetto antiterrorismo*, cit., p. 55 ss.

[156] In sede di lavori dell'Assemblea Costituente, Giovanni Leone osservò che si doveva rinunciare alla nobile aspirazione di un autonomo corpo di polizia giudiziaria alla dipendenza esclusiva dell'autorità giudiziaria, per le difficoltà insite nella creazione *ex* novo di un organismo speciale. Cfr. Resoconto stenografico delle sedute dell'Assemblea, p. 2530. Tuttavia, già a inizio del secolo scorso si affermava che «non si deve pericolosamente affidare l'azione repressiva alla stessa polizia di sicurezza, che non sa convenientemente esercitare l'azione preventiva». Così U. CONTI, *Della polizia giudiziaria*, in *Giust. pen.,* 1990, p. 138.

[157] Come sostenuto, «[C]convivenza funzionale in capo ai medesimi uomini che non può ritenersi casuale o determinata solo da cronici limiti d'organico, ma che risulta imposta dall'identità delle attività che svolgono e dei beni giuridici che tutelano». Così A. ZAPPULLA, *La formazione della notizia di reato*, cit., p. 252. Nello stesso senso, già P. TONINI, *Polizia giudiziaria e magistratura. Profili storici e sistematici,* cit., p. 271.

[158] In questo senso E. ANDOLINA, *Le intercettazioni e i controlli preventivi*, cit., p. 575.

agevolata soprattutto da quella collaborazione tra gli uomini di *intelligence* e quelli di polizia cui il legislatore nazionale ha mirato negli ultimi anni.

In effetti, la cooperazione tra *intelligence* e p.g., può agevolare un ingresso "indiretto" delle informazioni apprese *ante delictum*, quanto meno per indirizzare le indagini verso una "ricerca mirata"[159]: non è infrequente, infatti, che le investigazioni compiute "per" la formazione della notizia di reato da parte della p.g. siano "guidate" dagli uomini dell'*intelligence* che ottengono dati sospetti nell'ambito dell'attività di osservazione, informazione e vigilanza compiute durante i servizi di prevenzione[160], in quanto « […] nulla osta che [le notizie raccolte in sede preventiva] possano essere utilizzate in modo surrettizio quali occulti strumenti di indagine da cui poi origineranno atti investigativi *post delictum*, al contrario sicuramente utilizzabili»[161].

Si pensi, ad esempio, che sulla base delle notizie acquisite tramite intercettazioni preventive d'*intelligence*, pur non figurando negli atti di indagine, la polizia giudiziaria proceda a perquisizioni di propria iniziativa e, in esito ad essa, al sequestro del corpo del reato e delle cose ad esso pertinenti o all'arresto in flagranza o al fermo di indiziato di delitto[162].

Se, dunque, non può di fatto impedirsi che le notizie accolte in sede preventiva vengano – più o meno – indirettamente a conoscenza della polizia giudiziarie ed impiegate nelle successive indagini, sarebbe opportuno contenere il pericolo di un uso improprio delle operazioni in esame.

Intanto, nella piena consapevolezza di non poter rinunciare ad "elementi assai preziosi in virtù dei supremi interessi della giustizia"[163], parrebbe opportuno delineare una rigorosa disciplina circa il *modus operandi* dei soggetti legittimati alle "investigazioni preventive".

In questo senso, parrebbe auspicabile – non solo un "controllo esterno" da parte dell'autorità giudiziaria ma anche – l'introduzione di precise regole "interne" che consentano di istituire un «eguale paradigma investigativo»[164] che semplifichi la tracciabilità delle operazioni eseguite.

Per quanto riguarda più propriamente l'istituto delle intercettazioni preventive, un rimedio potrebbe derivare dalla previsione di un controllo di legalità non solo effettivo – ovvero ancorato a parametri oggettivi e concreti idonei a vincolare la discrezionalità applicativa e ad impedire che l'esecutivo, per il tramite della polizia di sicurezza, possa in qualche modo inserirsi nell'accertamento processuale – ma anche continuo, effettuato, cioè, oltre che al momento del rilascio dell'autorizzazione preventiva, anche *a posteriori*, durante l'espletamento dell'intera attività.

Solamente attraverso un controllo così congegnato «l'autorità giudiziaria sarebbe in condizione di riscontrare l'eventuale configurarsi di una notizia di reato; evenienza in cui dovrebbe venir meno l'ammissibilità dell'intercettazione preventiva e l'efficacia dell'ipotetico decreto autorizzativo»[165].

---

[159] Sul punto M.L. DI BITONTO, *Raccolta di informazioni e attività di* intelligence, cit., p. 255; G. SANTALUCIA, *Il potere del pubblico ministero*, cit., p. 155.

[160] In questo senso L. D'AMBROSIO, *Ruolo e attività della polizia giudiziaria nelle indagini: brevi considerazioni e qualche proposta*, in *Cass. pen*., 2006, f. 9, p. 2686 ss. Ma già, F. DE LEO, *Il pubblico ministero*, cit., p. 1442 s.

[161] Così L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 9.

[162] L'esempio è riportato da L. FILIPPI, *Terrorismo internazionale,* cit., p. 169.

[163] Così C. cost., 27 dicembre 1974, n. 300, cit.

[164] La predisposizione di adeguati protocolli operativi è proposta da D. CURTOTTI, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, cit., p. 448.

[165] Così E. ANDOLINA, *Le intercettazioni e i controlli preventivi,* cit., p. 576.

6. L'UTILIZZABILITÀ PROCESSUALE DEL MATERIALE CONOSCITIVO "PER" LA RICHIESTA DI INTERCETTAZIONI E CONTROLLI PREVENTIVI

Attenzione particolare merita la *quaestio* relativa alla presunta spendibilità processuale della mole di informazioni che entrano nel patrimonio conoscitivo del p.m. allorquando gli uomini d'*intelligence* presentano formale istanza per procedere alle intercettazioni e ai controlli preventivi sulle comunicazioni, *ex* art. 4, comma 2, l. 155/2005, così come sostituito dall'art. 12, l. 133/2012.

Come noto, all'esito del "ciclo investigativo d'*intelligence*" – procacciamento dei dati mediante tecniche di sorveglianza non mirata; incrocio degli stessi per l'individuazione di gruppi di relazione; esecuzione delle attività "tipiche" per individuare il sospetto –, gli uomini del DIS informano il p.m. dell'attività preventiva compiuta, anche attraverso la consegna del materiale idoneo a rappresentare l'informazione acquisita, al fine di permettergli di valutare l'indispensabilità delle operazioni di intercettazione preventiva.

Di qui le criticità. Ci si domanda, in sostanza, se quel "patrimonio conoscitivo" di cui entra in possesso il p.m. possa o meno trovare una qualche utilizzazione nell'ambito del processo penale "puro", ovvero, al contrario, debba seguire il medesimo trattamento delle informazioni apprese durante l'esecuzione delle captazioni e dei controlli preventivi di cui all'art. 226 disp. att. c.p.p.[166].

Al fine di trovare una soluzione all'enigma sono necessarie alcune considerazioni preliminari.

Intanto, la possibilità di utilizzare "prove precostituite", ossia redatte fuori dal procedimento penale ovvero prima ancora della sua instaurazione, è ormai pacifica sia in dottrina che in giurisprudenza, in ragione del condivisibile obiettivo di «non disperdere strumenti di conoscenza»[167].

In secondo luogo, va precisato che nessuna norma – né codicistica, né contenuta in leggi speciali – vieta l'acquisizione degli atti inerenti alle indagini proattive "atipiche" degli uomini d'*intelligence*[168]. Allo stato dell'arte, infatti, non è disciplinata la "sorte" risultanze delle attività prodromiche alla richiesta di cui all'art. 226 disp. att. c.p.p., ossia quelle investigazioni condotte dai Servizi di *intelligence* per procacciarsi gli elementi investigativi sui quali si fonda l'istanza e la conseguente decisione del p.m.

In effetti, il dettato normativo che impone l'inutilizzabilità (diretta e indiretta) del materiale acquisito in via preventiva (art. 226, comma 5 disp. att. c.p.p.) e la relativa distruzione dei verbali e supporti che quei dati contengono (art. 226, comma 3 disp. att. c.p.p.), inerisce solo ai risultati ottenuti dalle intercettazioni e dai controlli *ante delictum*, non estendendosi, per contro, al complesso di informazioni raccolte "per" fondare la richiesta autorizzativa.

Non solo. Seppur limitatamente alle informazioni apprese attraverso il duttile strumento della cooperazione internazionale, l'art. 6, d.lgs. 54/2015, rubricato "*Utilizzazione delle informazioni*

---

166 In relazione al più generale tema dell'inutilizzabilità delle prove nel processo penale come sanzione derivante da un'acquisizione illecita, *ex multis,* G. ARICÒ, *Riflessioni in tema di inutilizzabilità delle prove nel nuovo processo penale,* in *Annali dell'istituto di diritto e procedura penale (Università degli studi di Salerno),* 1993, p. 28 ss.; F. CORDERO, *Prove illecite nel processo penale,* Giuffrè, 1963, p. 55 ss.; ID, *Tre studi sulle prove penali,* Giuffrè, 1963, p. 71 s.; N. GALANTINI, *L'inutilizzabilità della prova nel processo penale*, Cedam, 1992, 144 ss. Più di recente, C. CONTI, *Accertamento del fatto e inutilizzabilità nel processo penale*, cit., p. 44 ss.; F. DINACCI, *L'inutilizzabilità nel processo penale. Struttura* e *funzione del vizio,* Giuffrè, 2008, p. 9 ss.

167 P. TONINI–C. CONTI, *Il diritto delle prove penali*, Giuffrè, 2014, p. 383.

168 Come rilevato, «[L]l'attività d'*intelligence* può costituire oggetto di accertamento penale […] in via principale. […] l'oggetto dell'istruzione è costituito dall'operato dei servizi: in tali circostanze l'autorità giudiziaria è chiamata ad attuare un sindacato di legalità penale». Così M. CAIANIELLO, *L'*intelligence *come oggetto di accertamento penale*, in AA. VV., *Nuovi profili del segreto di Stato e dell'attività di* intelligence, cit., p. 307.

o delle analisi come prova nell'ambito di un'indagine penale", prevede la possibilità di acquisire, previa autorizzazione dello Stato membro, i dati raccolti durante l'espletamento delle attività preventive d'*intelligence* «come prove o elementi di prova», nell'ambito del processo penale.

Inoltre, ai sensi dell'art. 256 *bis* c.p.p., è consentita l'acquisizione, da parte del p.m., di documenti e atti presso le sedi dell'AISI o dell'AISE o presso gli uffici del DIS, «qualora gli stessi risultino strettamente indispensabili ai fini delle indagini»[169], consentendo, *de facto,* l'utilizzo processuale dei risultati delle attività di indagine preventiva dei Servizi.

Da quanto detto, emerge che, a prescindere dal deposito formale degli elementi attestanti l'attività di *intelligence* preventiva da cui emergono gli elementi su cui fondare la richiesta di intercettazioni preventive, gli atti inerenti alle indagini proattive possono trovare precisa collocazione nel procedimento penale sulla base di una "scelta investigativa" del p.m.: infatti, qualora lo stesso non ricevesse materialmente tali documenti ma avendo comunque una conoscenza (indiretta) delle ragioni che supportano l'istanza a procedere, può personalmente recuperare quel materiale presso le sedi del DIS, dell'AISE o dell'AISI che diventano, *tout court,* elementi probatori da sottoporre alla valutazione del giudice.

Se questi sono gli indici dai quali emergono spiragli per consentire un utilizzo procedimentale alle informazioni preventive d'*intelligence*, si potrebbe per contro obiettare che le stesse trovino uno sbarramento processuale, in punto di acquisizione e di utilizzo, in ragione del vincolo del segreto di Stato apposto, *ex* art. 39, comma 1, l. 124/2007, «agli atti, documenti, notizie e attività la cui diffusione potrebbe recare danno all'integrità della Repubblica»[170].

Sotto questo profilo occorre precisare che le notizie apprese dagli uomini d'*intelligence* in ragione delle attività di informazione e sicurezza non sempre possono trovare un simile limite probatorio.

Più nel dettaglio, ai sensi del comma 11 dell'art. 39, l. 124/2007, non possono essere coperte dal segreto di Stato notizie relative a fatti eversivi dell'ordine costituzionale o concernenti il terrorismo, delitti di strage, associazione a delinquere di stampo mafioso, scambio elettorale politico–mafioso.

A ben guardare, le ipotesi delittuose or ora richiamate ineriscono ai "casi" per i quali la legge legittima l'esecuzione delle intercettazioni e dei controlli preventivi sulle comunicazioni, di cui all'art. 226 disp. att. c.p.p.; può, quindi, affermarsi che le informazioni apprese dai Servizi d'*intelligence* in relazione alla prevenzione dei reati di criminalità organizzata e terrorismo, non essendo vincolate dal segreto di Stato, possono trovare impiego procedimentale.

Una volta ammessa la trasmigrazione in fase processuale delle risultanze delle investigazioni proattive, pare opportuno individuarne la corretta veste giudica al fine di inquadrare la relativa acquisizione nel *genus* dei mezzi di prova tipici.

Si ritiene che alle notizie e ai dati acquisiti dai Servizi d'*intelligence* possa essere attribuita la forma di "documento", rispettandone i crismi fondamentali[171], costituendo «una rappresentazione

---

[169] Si esprime così F. GIUNCHEDI, *Le attività di prevenzione e di ricerca di* intelligence, cit., p. 10.

[170] Il segreto di Stato, disposto dal Presidente del Consiglio dei Ministri, impedisce all'autorità giudiziaria l'acquisizione e l'uso, anche indiretto, delle notizie sottoposte a tale vincolo. In particolare, ai sensi dell'art. 203 c.p.p., «[I]i pubblici ufficiali, i pubblici impiegati e gli incaricati di un pubblico servizio hanno l'obbligo di astenersi dal deporre su fatti coperti dal segreto di Stato. Se il testimone oppone un segreto di Stato, l'autorità giudiziaria ne informa il Presidente del Consiglio dei ministri, ai fini dell'eventuale conferma, sospendendo ogni iniziativa volta ad acquisire la notizia oggetto del segreto». Sul tema, AA. VV., *I servizi di informazione e il segreto di Stato*, cit., *passim*; C. BONZANO, *Segreto di Stato e prova penale*, in *Il Libro dell'anno del diritto*, Treccani, 2015, p. 617 ss.; ID., *Il segreto di Stato nel processo penale,* Cedam, 2010, p. 68 ss.

[171] Il concetto di documento comprende quattro elementi fondamentali: il fatto rappresentato (fatti, persone, cose o dichiarazioni); la rappresentazione (ossia la sua riproduzione); l'incorporamento (la rappresentazione fissata su un supporto attraverso metodo analogico o digitale); la base materiale

di conoscenza incorporata su qualsiasi base materiale, redatta da soggetti estranei al procedimento penale»[172].

In effetti, la scelta di fornire una simile qualificazione giuridica alla mole di informazioni raccolte *ante delictum*, può trovare conferme nel disposto dell'art. 220 disp. att. c.p.p.[173] che, in relazione agli atti compiuti dalle forze dell'ordine prima dell'acquisizione della *notitia criminis*, attribuisce ai dati raccolti in una fase pre–procedimentale la forma di "documenti"[174].

Conseguentemente, l'acquisizione processuale di tali dati seguirà le regole generali relative alle prove documentali[175] che, come noto, non risultano sottoposte ai termini di cui all'art. 493 c.p.p.[176].

(il supporto su cui è incorporata la rappresentazione). Come precisato nella Relazione al progetto preliminare (p. 67) e nella Relazione al testo definitivo (p. 182), gli artt. 234 ss. riguardano solo «i documenti formati fuori del processo nel quale si richiede o si dispone che essi facciano ingresso». Nello stesso senso anche la giurisprudenza di legittimità, per cui «ai fini dell'ammissione delle prove documentali sono necessarie due condizioni: che il documento risulti formato fuori dal procedimento; che lo stesso oggetto della documentazione extraprocessuale appartenga al contesto del fatto oggetto di conoscenza giudiziale e non al contesto del procedimento». Sez. un., 28 marzo 2006, n. 26795, in *questa rivista,* 2006, p. 3937 ss., con nota di RUGGIERI, *Riprese visive e inammissibilità della prova.*

[172] Così P. TONINI–C. CONTI, *Il diritto delle prove penali*, cit., p. 353.

[173] L'art. 220 disp. att. c.p.p. sottolinea la differenza tra documento e documentazione, stabilendo che qualora un organo di vigilanza assuma la qualifica di p.g., dal momento in cui iniziano ad emergere degli indizi di reità, non redige più "documenti" ma "documentazione". In relazione alla distinzione tra documento e documentazione, che, per converso, è un atto del procedimento, cfr. Corte cost., 4 dicembre 2009, n. 320, in *Giur. cost*., 2009, p. 4810, con nota di M. VILLANI, *La Corte ribadisce i rapporti tra legalità costituzionale, legalità sostanziale e legalità processuale*. Sul punto A. CORBO*, I documenti*, in AA. VV., *Trattato di procedura penale*, cit., p. 371 ss.; L. KALB, *Il documento nel sistema probatorio*, Giappichelli, 2000, p. 16; A. LARONGA, *La prova documentale nel processo penale,* Giappichelli, 2004; P. MAGGIO, voce *Prova documentale,* in *Enc. giur*., XXIV, Treccani, 1990, p. 1; F. ZACCHÈ, *La prova documentale,* Giuffrè, 2012. Se il documento rappresenta un fatto o un atto differente dall'atto processuale compiuto nel procedimento nel quale il documento è acquisito, la documentazione è un atto processuale compiuto nel medesimo procedimento. In dottrina, G. MEZIO, sub *art. 220 disp. att. c.p.p.*, in *Codice di procedura penale commentato*, cit., p. 8816 ss.

[174] Secondo la giurisprudenza di legittimità, gli atti compiuti prima del sorgere degli indizi di reato devono essere considerati documenti a tutti gli effetti. Cass., sez. IV, 28 aprile 2006, n. 3554, in *Arch. Giur. circ.,* 2007, f. 4, p. 378 ss. In dottrina, M. NOBILI, *Atti di polizia amministrativa utilizzabili nel processo penale e diritto di difesa: una pronuncia marcatamente innovativa*, in *Foro it.,* 1984, f. I, p. 374.

[175] Sul punto, per tutti, G. UBERTIS, *Documenti e oralità nel nuovo processo penale*, in *Studi in onore di Giuliano Vassalli. Evoluzione del diritto e della procedura penale,* a cura di M.C. Bassiouni–A.R. Latagliata–A.M. Stile, *Politica criminale e criminologia. Procedura penale*, Giuffrè, 1991, p. 3030 ss. Più di recente, R. ADORNO, *L'ammissione della prova in dibattimento*, Giappichelli, 2012; E.M. MANCUSO, *Il regime probatorio dibattimentale,* Giuffrè, 2017, p. 105 ss.; O. MAZZA, *Le insidie al primato della prova orale rappresentativa. L'uso dibattimentale di materiale probatorio precostituito*, in *Riv. it. dir. proc. pen.*, 2011, p. 1533 ss.

[176] Ad avviso dei giudici di legittimità, «deve escludersi che l'art. 493 […] preveda una preclusione alla esibizione di documenti, ed all'ammissione di essi da parte del giudice, ad un momento successivo a quello fissato dalla norma suddetta, essendo tale preclusione esplicitamente limitata alle prove che devono essere indicate nelle liste di cui all'art. 468 c.p.p.», fermo restando che le altre parte hanno il diritto di esaminarli a norma dell'art. 495, comma 3 c.p.p.». Cass., sez. II, 22 novembre 1994, n. 2533, in *Cass. pen.,* 1996, f. 2, p. 844.

Più in particolare, nel caso di atti non aventi contenuto dichiarativo[177], i documenti contenuti nel fascicolo del p.m. possono confluire in quello dibattimentale attraverso due differenti modalità: sia a seguito della produzione e contestuale deposito ad opera della parte che intende introdurre il documento nel corso dell'udienza, ai sensi del disposto di cui all'art. 495, comma 3 c.p.p.[178], sia mediante acquisizione concordata, *ex* art. 493, comma 3 c.p.p., per cui risulta sanata l'inutilizzabilità di tipo fisiologico[179].

Nel caso di documenti aventi contenuto dichiarativo[180], invece, l'acquisizione può avvenire mediante la testimonianza consentita anche agli uomini d'*intelligence* che possono servirsi di identità mascherate[181].

---

[177] Sul concetto di documenti non aventi contenuto dichiarativo, Cass., sez. I, 13 luglio 2012, n. 42130, in *C.E.D. Cass*., n. 253800; sez. III, 16 aprile 2008, n. 19968*, ivi,* 240048; sez. V, 8 ottobre 2003, n. 44868, *ivi* n. 227009; sez. III, 15 giugno 1999, n. 11116, *ivi*, 214457. Come sostenuto dalla più recente giurisprudenza di legittimità, «[I]i rilievi fotografici rappresentativi dello stato dei luoghi, nozione rientrante nella categoria delle "cose" contemplata dall'art. 234, comma primo, c.p.p. rientrano a pieno titolo nelle prove documentali che, avendo contenuto figurativo, non costituito cioè dalla scrittura, bensì dalle immagini, costituiscono di per sé piena prova che può essere sempre acquisita e sulla quale il giudice può validamente fondare il proprio convincimento». Così, sez. III, 4 maggio 2018, n. 19139, in *Arch. pen*., 16 maggio 2018.

[178] Ai sensi dell'art. 495, comma 3 c.p.p. «[P]prima che il giudice provveda sulla domanda, le parti hanno la facoltà di esaminare i documenti di cui è richiesta l'ammissione». La scelta di far coincidere il momento di ammissione del documento con la sua acquisizione deriva da questioni di ordine pratico: mentre per la prova testimoniale e peritale sono necessari tempi tecnici per la citazione dei soggetti chiamati a deporre, l'esigenza di anticipazione non sussiste per la prova documentale. Tuttavia, la norma chiarisce che le parti hanno la facoltà di esaminare le prove documentali di cui è stata richiesta l'ammissione; di conseguenza «il giudice dovrà dare alle parti un tempo congruo in relazione alla quantità e alla complessità dei documenti da esaminare». Così DA. E CARO, *Ammissione e formazione della prova in dibattimento*, in AA. VV., *La prova penale,* cit., p. 375. Sul punto anche, E. ANDOLINA, *Gli atti anteriori all'apertura del dibattimento*, Giuffrè, 2008, p. 123 ss. Nello stesso senso anche la giurisprudenza di legittimità, per cui la sentenza che utilizza i documenti acquisiti su richiesta del p.m. senza disporre la rinnovazione è affetta da nullità di cui all'art. 178, lett. *c*., c.p.p. Cfr. Cass., sez. VI, 6 novembre 2011, n. 30897, in *C.E.D. Cass.,* n. 265599.

[179] Su cui, *ex multis,* R. DORNO, *Ammissione delle prove*, in AA. VV., *Trattato di procedura penale*, cit., p. 172 ss.; G. ILLUMINATI, *Ammissione e acquisizione della prova nell'istruzione dibattimentale*, in AA. VV., *La prova nel dibattimento penale*, a cura di P. Ferrua– F.M. Grifantini–G. Illuminati–R. Orlandi, Giappichelli, 2007, p. 93 ss. Nello stesso senso la più recente giurisprudenza di legittimità. Cfr. Cass., sez. VI, 7 ottobre 2016, n. 48949, in *C.E.D. Cass*., n. 268213.

[180] Secondo un orientamento ormai pacificamente superato grazie all'apporto chiarificatore della giurisprudenza costituzionale, nella nozione di "documenti" non possono rientrare quelli avente contenuto dichiarativo, non potendo essere utilizzati come prova del fatto narrato «in quanto contrario al principio di oralità». Così NAPPI, *Guida al codice di procedura penale*, Giuffrè, 1995, p. 350. In quella circostanza, la Consulta ha chiarito che il documento contenente una dichiarazione può costituire prova del fatto rappresentato ma, laddove l'accusato richieda, a controprova, l'escussione del soggetto che ha reso la dichiarazione contenuta nel documento, e ciò non avvenga per scelta del dichiarante, il documento è inutilizzabile *ex* art. 526 comma, 1 *bis* c.p.p. Corte cost., 30 marzo 1992, n. 142, in *Riv. it. dir. proc. pen.,* 1993, p. 361.

[181] Trattasi delle cc.dd. attività sotto coperture svolte dai servizi di informazione e sicurezza, che si differenziano dall'omologa attività eseguibile anche dalle forze di polizia in quanto non finalizzate all'accertamento dei fatti di reato ma solo alla loro neutralizzazione. In assenza di una specifica definizione normativa, la locuzione indica un complesso di attività investigative nelle quali una persona – un ufficiale della polizia giudiziaria o un privato cittadino – celando la propria identità, si infiltra all'interno di organizzazioni criminali allo scopo di scoprirne la struttura, sottrarle risorse essenziali, denunciare i partecipanti. Per una ricostruzione storica dell'istituto, C. DE MAGLIE, *L'agente provocatore. Un'indagine dommatica e politico-criminale,* Giuffrè, 1991. Più di recente,

Da quanto detto emerge che l'attività tipica dei Servizi di informazione e sicurezza può fare ingresso nel procedimento penale attraverso i "tradizionali" canali di acquisizione delle prove documentali, determinando «l'ennesimo scivolamento all'indietro sino ai territori dell*'intelligence* [che] rischia di alimentare l'accertamento con dati di origine occulta, di nascondere circostanze viceversa preziose nel lumeggiare il contesto investigativo di scoperta dei fatti illeciti, si sottrarre ulteriore presa allo stesso pubblico ministero e persino alla polizia, consegnando, così, il primato nelle mani dei servizi segreti: saremmo dunque di fronte […] alla "*Vergeheimdienstlinchung*" del processo penale»[182].

7. La raccolta preventiva dei dati alla prova dei principi dello Stato di diritto

Dall'esegesi della normativa dettata in materia di intercettazioni e controlli preventivi sulle comunicazioni, emerge che le regole predisposte dal legislatore dell'88 e poi ritoccate nel corso degli anni, risultano assai più blande e meno stringenti rispetto a quelle più rigorose previste dal legislatore per le captazioni giudiziarie, giustificando tale scelta in ragione dell'inutilizzabilità procedimentale e processuale dei dati raccolti in fase preventiva.

Sennonché, se l'innegabile eterogeneità dell'istituto può comportare un affievolimento di tutela dei diritti fondamentali coinvolti, non può condurre ad uno svuotamento delle garanzie e dei principi cardine dello Stato di diritto, quali quello di legalità, tassatività e determinatezza, sussidiarietà ed *extrema ratio*[183]; principi, questi, che «rappresentano il livello di tutela irrinunciabile al di sotto del quale l'attività di prevenzione non appare più ragionevole e, pertanto, tollerabile»[184].

Allo state dell'arte, dunque, appare troppo semplicistica la soluzione per cui sarebbe possibile estendere le considerazioni già ampiamente svolte in tema di captazioni processuali anche alle intercettazioni preventive, senza soffermarsi sui tratti peculiari di un istituto che si profila assai più ingerente nella vita privata dei soggetti coinvolti.

E ciò per motivi di natura ontologica e ideologica.

Intanto, sul piano del bilanciamento degli interessi, le intercettazioni e i controlli *ante delictum* determinano una limitazione al godimento dei diritti inviolabili dell'uomo senza una legittimazione ancorabile alla necessità di repressione di un fatto di reato. Va da sé che, in assenza di ipotesi di reato, il limite di tollerabilità alla menomazione delle prerogative individuali appare assai più ristretto rispetto a quanto accade a seguito dell'istaurazione del procedimento penale,

---

senza pretese di completezza, si rinvia a P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni "sotto copertura", captazione di dati digitali*, in *Riv. dir. proc.,* 2010, p. 795, secondo cui «[U]un'analoga commistione tra profilassi e repressione si realizza per effetto dell'"infiltrazione" di agenti all'interno delle organizzazioni criminali e delle attività *under cover*, nonché in conseguenza della captazione di dati digitali». Da ultimo, D. CURTOTTI, *Operazioni sotto copertura*, in AA. VV., *Le associazioni di tipo mafioso*, a cura di B. Romano, Utet, 2015, p. 427 s. La deposizione con l'uso di generalità di copertura rappresenta una delle novità introdotte dall'art. 8 del d.l. 7/2015 che, operando una modifica del comma 2 *bis* dell'art. 497 c.p.p., consente – anche al personale dei servizi di informazione – l'utilizzazione delle generalità di copertura in sede di esame testimoniale. Sul punto, D. CURTOTTI, *Operazioni sotto copertura*, cit., p. 427 ss.

[182] Così D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico),* cit., p. 51.

[183] Sul punto, autorevolmente, A. MALINVERNI, *Principi del processo penale*, Giappichelli, 1972, p. 210 ss.

[184] Si esprime così E. ANDOLINA, *Le intercettazioni e i controlli preventivi,* cit., p. 572.

dal momento che l'interesse contrapposto all'intrusione si mostra evanescente e dai contorni poco chiari e definiti[185].

Inoltre, nel *genus* delle intercettazioni preventive rientrano altre attività investigative che poco o nulla hanno in comune con la captazione di conversazioni e comunicazioni, finendo per rappresentare strumenti di controllo e sorveglianza.

Più in particolare, la norma legittima il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione di dati esterni relativi alle comunicazioni telefoniche e telematiche e di ogni altra informazione utile ai fini preventivi[186]; tutte attività che risultano ancora più invasive della sfera privata degli individui rispetto alle intercettazioni *strictu sensu* intese.

La verifica della compatibilità dell'istituto *de quo* rispetto all'assetto costituito sembra ancor più complessa allorquando gli operatori si avvalgono di strumenti tecnici altamente qualificati: a fronte delle indiscriminate prestazioni che il captatore informatico, almeno in potenza, può realizzare, è inevitabile che l'intrusione nella sfera intima della persona controllata si manifesta in una misura finora sconosciuta, tanto profonda quanto pervasiva, a tal punto da «rasenta[rne] il crollo psichico»[187].

Ecco la ragione per cui l'intrusione informatica esige una nuova e più specifica riflessione del giurista; come sostenuto, «[…] lo strumento captativo […] è più intrusivo delle ordinarie intercettazioni [dal momento che] si opera a cavallo tra intercettazioni e nuove forme di "mezzo di ricerca di prova atipica", priva però dei requisiti della giurisdizionalità specificamente richiesti, invece, per la prova atipica"»[188].

Quando lo strumento viene impiegato nelle indagini proattive, la limitazione alle libertà positive risulta ancor meno tollerabile di quanto accade nelle intercettazioni giudiziarie, pur se condotte mediante captatore. A ben guardare, infatti, sul piano del bilanciamento degli interessi, le investigazioni *ante delictum* determinano una limitazione al godimento dei diritti inviolabili dell'uomo senza una legittimazione ancorabile alla necessità di repressione di un fatto di reato. Va da sé che, in assenza di ipotesi di reato, il limite di tollerabilità alla menomazione delle prerogative individuali appare assai più ristretto rispetto a quanto accade a seguito dell'istaurazione del procedimento penale, dal momento che l'interesse contrapposto all'intrusione si mostra evanescente e dai contorni poco chiari e definiti[189].

Ancor più seri appaiono i rischi di lesione dei principi fondamentali dello Stato democratico quando il captatore informatico viene impiegato dai Servizi di *intelligence* per condurre attività di sorveglianza di massa.

L'acquisizione della mole di dati in fase preventiva realizza una schedatura e un controllo sistemico di dati non motivato dall'emersione di indizi a carico dei soggetti monitorati, determinando la violazione dei *dicta* europei che, quale parametro di legalità delle operazioni di captazione, impongono l'individuazione e l'identificazione dei controllati[190]. Ciò non solo perché

---

[185] In questo senso L. FILIPPI–M.F. CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 4.

[186] L'art. 226, comma 4, disp. att. c.p.p., in alternativa o congiuntamente alle intercettazioni, prevede che «con le modalità e nei casi di cui ai commi 1 e 3, può essere autorizzato il tracciamento delle comunicazioni telefoniche e telematiche, nonché l'acquisizione di dati esterni relativi alle comunicazioni telefoniche e telematiche intercorse e l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni».

[187] L'espressione appartiene a P. TONINI–CC. ONTI, *Il diritto delle prove penali*, cit., p. 482.

[188] GRIFFO, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore*, in *Dir. pen. cont*., 2018, n. 2, p. 43.

[189] In questo senso L. FILIPPI–M.F.CORTESI, voce *Intercettazione preventiva di comunicazioni*, cit., p. 4.

[190] CGUE, Grande Camera, 8 aprile 2014, *Digital Rights Ireland e Seitlinger,* cause riunite C–293/12 e C–595/12, § 33–36, secondo cui «una normativa che consenta alle autorità pubbliche di accedere in

le limitazioni alle libertà fondamentali possono avvenire quanto meno in presenza di elementi indiziari che ne giustificano la compressione[191], ma anche e soprattutto al fine di consentire al soggetto passivo identificato la possibilità di accertare la correttezza dell'esecuzione delle attività espletate in concreto[192].

Da quanto detto emerge che il *vulnus* determinato dagli strumenti tecnici di monitoraggio in fase preventiva si spinge ben oltre la violazione delle prerogative individuali, finendo per collidere con i principi fondanti l'assetto costituito.

In primis, l'assenza di qualsivoglia "sospetto" quale presupposto per procedere all'acquisizione massiva dei dati e alla successiva analisi determina una potenziale interferenza con la presunzione di innocenza[193], di cui all'art. 27, comma 2 Cost.[194], qui da intendersi quale "regola universale di trattamento"[195], nel senso che l'individuo non deve essere assimilato

---

maniera generalizzata ai dati personali, pregiudica i diritti al rispetto della vita privata ed alla protezione dei dati, indipendentemente dal se le informazioni abbiano o meno carattere sensibile o che gli interessati abbiano subito eventuali inconvenienti in seguito a tale ingerenza».

[191] Come ha di recente precisato la Corte EDU, sussiste una violazione dell'art. 6, comma 2 CEDU tutte le volte in cui l'autorità giudiziaria non ha indicato in maniera esaustiva i motivi che hanno determinato la compressione delle libertà fondamentali. Corte EDU, 26 giugno 2016, *Mugosa c. Montenegro*, n. 76522/12; Corte EDU, 10 novembre 2015, *Slavov e altri c. Bulgaria*, n. 58500/10.

[192] Corte EDU, sez. IV, 29 marzo 2005, *Matheron c. Francia*, n. 57752/00, § 40; Corte EDU, Grande Camera, 24 aprile 1990, n. 11801/85, *Kruslin c. Francia*, n. 11801/85; Corte EDU, Grande Camera, 26 marzo 1987, *Leander c. Svezia*, n. 9248/81.

[193] Sulla presunzione di innocenza, *ex multis*, F. CARNELUTTI, *Principi del processo penale*, Jovene, 1960, p. 159 ss.; M. FERRAIOLI, voce *Presunzione (dir. proc. pen.),* in *Enc. dir.,* XXXV, Giuffrè, 1986, p. 304 ss.; P.P. PAULESU, voce *Presunzione di non colpevolezza*, in *Dig. disc. pen.*, VIII, Utet, 1995, p. 670 ss.; V. GAROFOLI, *Presunzione d'innocenza e considerazione di non colpevolezza. La fungibilità delle due formulazioni,* in AA. VV., *Presunzione di non colpevolezza e disciplina delle impugnazioni*, Giuffrè, 2000, p. 98 ss.; G. ILLUMINATI, voce *Presunzione di non colpevolezza,* in *Enc. giur.,* XXIV, Treccani, 1991, p. 2 ss.; ID*., La presunzione d'innocenza dell'imputato*, Il Mulino, 1979. Più di recente, F. GIUNCHEDI, *La tutela dei diritti umani nel processo penale*, Cedam, 2007, p. 66 ss.; E. MARZADURI, *Considerazioni sul significato dell'art. 27 comma 2, Cost.: regola di trattamento e regola di giudizio*, in AA. VV., *Processo penale e Costituzione*, a cura di F. Dinacci, Giuffrè, 2010, p. 314 ss.; C. FIORIO, *La presunzione di non colpevolezza*, in AA. VV., *Fisionomia costituzionale del processo penale*, a cura di G. Dean, Giappichelli, 2007, p. 120 ss.; P.P. PAULESU, *La presunzione di non colpevolezza dell'imputato*, Giappichelli, 2009.

[194] Il principio della "non colpevolezza fino a prova contraria" è riconosciuto anche in ambito europeo. In particolare, è contemplato nell'art. 6, comma 2 CEDU, ai sensi del quale «ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia legalmente accertata», nonché nell'art 48 della Carta dei diritti fondamentali dell'Unione europea, per cui «ogni imputato è considerato innocente fino a quando la sua colpevolezza non sia legalmente provata». Infine, sul piano internazionale, il principio è tutelato dal secondo comma dell'art. 14 del Patto internazionale sui diritti civili e politici, secondo cui «ogni individuo accusato di un reato ha il diritto di essere presunto innocente sino a che la sua colpevolezza non sia stata provata legalmente». Sul punto, *ex plurimis*, S. BUZZELLI–R. CASIRAGHI–F. CASSIBBA–P. CONCOLINO–L. PRESSACO, *Diritto a un equo processo,* in AA. VV., *Corte di Strasburgo e giustizia penale,* a cura di G. UBERTIS–F. VIGANÒ, Giappichelli, 2016, p. 161 ss.; A. DE CARO, *Presunzione d'innocenza, oneri probatori e regole di giudizio*, in AA. VV., *Procedura penale e garanzie europee*, a cura di A. Gaito, Giappichelli, 2006, p. 407 ss.; E. MARZADURI, *Presunzione di innocenza e tutela della libertà personale dell'imputato nella giurisprudenza della Corte europea dei diritti dell'uomo,* in AA. VV, *I principi europei del processo penale,* a cura di A. Gaito, Dike, 2016, p. 162 ss.; O. MAZZA, *Presunzione di innocenza e diritto di difesa,* in AA. VV., *I nuovi orizzonti della giustizia penale europea,* Giuffrè, 2015, p. 141 ss.

[195] G. ILLUMINATI, voce *Presunzione di non colpevolezza,* cit., p. 2.

nemmeno ad un potenziale indiziato e, dunque, subire restrizioni al godimento dei diritti fondamentali prima dell'istaurazione del rito penale.

Pur ammettendo, il nostro sistema, forme di limitazione alle libertà personale, queste risultano essere giustificate dalla sussistenza di un provvedimento giurisdizionale che valuta la pericolosità del soggetto raggiunto dalla misura, nei cui confronti sono già emersi gravi indizi di colpevolezza circa il compimento di un reato grave.

In questa circostanza, per contro, ogni individuo viene trattato con un pre–giudizio di pericolosità; ogni persona potrebbe trasformarsi in un potenziale sospetto della commissione di reati futuri e, di conseguenza, subire misure incidenti sui diritti di libertà solo in ragione della rispondenza a predeterminati (ma sconosciuti) "criteri di rischio" individuati dai Servizi di *intelligence*[196].

Ma ciò che desta maggiori perplessità è l'assenza di qualunque forma di regolamentazione delle "investigazioni proattive digitali"; *vacatio legis,* questa, che sottende una precisa scelta di politica criminale del legislatore nazionale il quale, intenzionalmente, lascia avvolta dal mistero una fase che solo formalmente esula dall'interesse processuale in senso stretto.

Più nel dettaglio, la "libertà" di azione delle Forze di polizia degli uomini d'*intelligence*, sia in relazione all'amorfo *modus operandi* che in relazione alla scelta discrezionale dei *target* per la selezione dei gruppi da monitorare, crea punti di frizione con il più generale principio di legalità[197], inteso quale diritto del singolo di conoscere le ragioni per le quali subisce una restrizione alla sua sfera di libertà, nonché le modalità con cui la stessa si realizza.

[196] È ben noto che l'individuazione di un soggetto quale possibile autore del reato attraverso l'utilizzo della profilazione può provocare un «fenomeno di distorta interpretazione di ogni fonte di prova in senso convergente con l'avvenuta identificazione su base criminologica del soggetto», in un'ottica di «raccolta degli elementi probatori selettiva, ossia volta a corroborare una sola posizione, negando le altre». Così L. LUPARIA, *Il* profiling *dell'autore del reato*, in AA. VV., *Le indagini atipiche*, I ed., cit., p. 340.

[197] Sul principio di legalità quale precetto fondante lo Stato di diritto, senza pretese di completezza, N. BOBBIO, *Principi generali di diritto*, in *Noviss. dig. it.*, XIII, Utet, 1966, p. 887 ss.; H. KELSEN, *Teoria generale del diritto e dello stato*, Etas, 1954, p. 261 s.; G. VASSALLI, *I principi generali del diritto nell'esperienza penalistica*, in *Riv. it. dir. proc. pen*., 1991, p. 701.

L'INDISPENSABILITÀ DELLA PREDETERMINAZIONE PER LEGGE DELL'INTRUSIONE INFORMATICA

Una volta attraversati gli impervi percorsi tracciati dall'esecuzione delle attività investigative condotte mediante captatore informatico sia in fase repressiva che preventiva e affrontati gli inevitabili risvolti processuali che ne derivano, possono trarsi alcune considerazioni che, prendendo le mosse dalla normazione vigente, si spingono fino ad avanzare soluzioni giuridiche inedite.

In prospettiva *de jure conditio*, la *quaestio* relativa all'impiego del *virus* informatico nel circuito processuale è stata affrontata spasmodicamente dal legislatore solo con precipuo riferimento alle intercettazioni di conversazioni e comunicazioni tra presenti, di cui all'art. 266, comma 2 c.p.p., quasi come se questa forma di captazione legalizzata fosse l'unica esperita o esperibile ricorrendo al diabolico strumento *de quo* e sulla quale si fonda il precario equilibrio tra le esigenze di sicurezza individuale e collettiva e la protezione dei diritti individuali fondamentali.

Il legislatore nazionale, in spregio al *trend* normativo internazionale ed europeo che si pone l'obiettivo di legalizzare le altre forme di "controllo" che pur possono realizzarsi attraverso l'ausilio di sofisticati strumenti investigativi, scientemente decide di non disciplinare le "altre" attività strettamente connesse all'utilizzo del *virus* informatico sia dai Servizi di *intelligence* per scopi di sicurezza che dalle Forze di polizia per corroborare la notizia di reato.

Soluzione semplicistica, questa, funzionale a placare l'inquietudine di quanti si approcciano al tema *de qua* interrogandosi sulla portata delle investigazioni "atipiche" condotte tramite *Trojan* e sul destino della mole di dati e delle informazioni canalizzate nell'etere digitale, acquisite sia al fine di anticipare le "tendenze" criminogene e neutralizzare il compimento del fatto di reato, sia per facilitare la ricostruzione dell'evento delittuoso e l'individuazione del colpevole.

Come ormai noto, l'incondizionato e incontrollato impiego del captatore informatico nelle indagini processuali tradizionali e nelle investigazioni proattive determina conseguenze assai pericolose per l'assetto costituito. Le ricadute sul terreno dei diritti sono piuttosto intuitive, quantomeno sotto il profilo dell'esistenza di indiretti condizionamenti e anomale restrizioni all'esercizio delle più basiche libertà personali. Altrettanto preoccupanti appaiono gli impieghi trasversali del captatore che consentono di condurre qualunque altra attività investigativa, pur non espressamente contemplata dal legislatore. Senza sottacere, poi, delle *quaestiones* legate all'uso indiretto della mole dei dati acquisiti in fase preventiva (sia nell'ambito delle intercettazioni preventive che nella sorveglianza di massa) all'interno del processo penale puro.

Di qui, il silenzio del legislatore, combinato alla mutevolezza delle posizioni giurisprudenziali sul tema, deve inquietare la comunità scientifica a fronte degli innegabili risvolti procedimentali e dell'evidente compressione dei diritti costituzionalmente garantiti che derivano dall'esecuzione del complesso di attività

comunque esperibili mediante captatore informatico e che, è bene ribadirlo, pur non trovando alcuna fonte normativa (né tipica, né atipica), risultano ampiamente utilizzati dagli organi inquirenti.

Avanzare proposte *de jure condendo* e intravedere soluzioni adeguate a contemperare le esigenze di sicurezza, tutela delle prerogative individuali e rispetto delle regole su cui si fonda il processo penale, non è cosa agevole, perché rischia di scivolare in una realtà astratta e poco concreta. Ma il giurista non può rimanere inerte, dovendo "scendere nell'arena" dove il diritto processuale penale deve fare i conti con le resistenze culturali di un sistema che intravede nella sicurezza collettiva l'unico valore per cui vale la pena di comprimere i diritti e i valori individuali.

L'individuazione di soluzioni e rimedi per arginare lo strapotere della tecnologia nella prevenzione e nell'accertamento dei reati, impone all'interprete di considerare, *in primis*, la compatibilità dei sistemi informatici di acquisizione dei dati con il sistema processuale.

In questo senso, l'indagine non può che partire da una considerazione piuttosto categorica ma assolutamente aderente alle logiche del processo accusatorio: qualora lo strumento sia impiegato per usi diversi da quelli espressamente contemplati dal legislatore deve ritenersi che i dati acquisiti diano luogo ad una prova incostituzionale, in quanto offrono al processo elementi «raccolti con modalità non disciplinate dal codice di rito e lesive dei diritti dell'individuo» (V. Grevi, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost*., 1973, p. 341), e di essi non dovrebbe essere fatto alcun uso, ancorché indiretto, nel corso del procedimento (C. Conti, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen., proc.,* 2018, n. 9, p. 1213 s.).

Occorre, tuttavia, prendere atto che, pur violando diritti fondamentali, i risultati ottenibili attraverso l'utilizzo di tali strumenti sono efficacissimi nella prevenzione e nella persecuzione del crimine, per cui non è prospettabile che il sistema rinunci a fare tesoro di un materiale probatorio così utile processualmente in quanto scevro da condizionamenti di ogni genere. Al contempo, però, bisogna mantenere ferma la consapevolezza dei costi, elevatissimi, che ciò comporta in termini di sacrificio delle garanzie individuali.

L'utilità delle investigazioni avanguardistiche non può e non deve giustificare ogni forma di violazione ai diritti e alle libertà fondamentali: se l'innegabile eterogeneità dell'istituto può comportare un affievolimento di tutela dei diritti fondamentali coinvolti, non può condurre ad uno svuotamento delle garanzie e dei principi cardine dello Stato di diritto, quali quelli di legalità, tassatività e determinatezza, sussidiarietà ed *extrema ratio*; principi, questi, che «rappresentano il livello di tutela irrinunciabile al di sotto del quale l'attività di prevenzione non appare più ragionevole e, pertanto, tollerabile» (A. Malinverni, *Principi del processo penale*, Utet, 1972, p. 210 ss.).

Il problema, allora, è quello di giungere ad un equilibrio tra l'esigenza di garantire la fruttuosità delle indagini, grazie all'utilizzo di una metodologia particolarmente efficace, e quella di non vanificare la tutela dei fondanti valori di libertà dell'individuo, propri di uno Stato democratico e connaturati alla Carta costituzionale.

Nella frenetica ricerca di un non sempre agevole compromesso, non sarebbe proficuo perseguire la strada dell'espunzione della scienza e della tecnica dal sistema, anelando un processo "puro" e scevro da contaminazioni esterne. Si rischierebbe di far perdere al

processo il suo naturale legame con la realtà. Di conseguenza, sembrerebbe opportuno consentirne un accesso "contingentato", al fine di bilanciare le esigenze investigative con la protezione dei diritti individuali. In altri termini, non è impiego del captatore informatico ad essere oggetto di critica, ma l'abuso, ossia il ricorso smodato agli strumenti *de quibus* che, secondo l'originaria *voluntas legis*, avrebbe dovuto rappresentare un *extrema ratio,* cui ricorrere allorquando gli altri sistemi di indagini risultano inefficaci allo scopo perseguito: l'uso "parsimonioso" del mezzo in esame, potrebbe rappresentare un primo passo per il raggiungimento dell'equilibrio tra sicurezza e diritti individuali.

Tuttavia, non essendo ipotizzabile lasciare alla disponibilità degli inquirenti la scelta di utilizzare "nuovi" ed invasivi strumenti d'indagine e nemmeno legittimare il suo impiego in sede giurisprudenziale attraverso interpretazioni estensive in una materia governata da un rigido principio di tassatività, sarebbe indispensabile predeterminare le modalità della nuova forma investigativa, tanto in fase preventiva che repressiva.

Da ciò deriva la necessità che il legislatore ridefinisca la materia in modo da renderla conforme ai principi europei, che impongono chiarezza, sufficienza, determinatezza della fattispecie nonché, in particolare, il rispetto del principio di proporzionalità. Una regolamentazione in forma chiara e compiuta sia delle singole attività esperibili che dei casi in cui l'intrusione informatica possa risultare legittima, risulterebbe funzionale alla tutela del principio di legalità nonché a conferire certezza al diritto di difesa, in modo da permettere al controllato di avere effettiva cognizione delle modalità di ingerenza degli investigatori nella sfera di riservatezza individuale, valutando la rispondenza dell'attività compiuta rispetto ai limiti individuati dal tenore della disposizione e dal contenuto del decreto autorizzativo.

Prima facie, si potrebbe prospettare una soluzione "radicale", un intervento riformatore che consenta di innovare completamente la disciplina *de qua* attraverso la normazione di tutte le singole attività esperibili dall'agente intrusore e la legalizzazione dell'impiego del *virus* informatico anche per compiere intercettazioni e controlli preventivi sulle comunicazioni.

Più nel dettaglio, in ragione della legittimazione giurisprudenziale all'esecuzione di intercettazioni telematiche mediante *virus* informatico (Cass., sez. V, 30 maggio 2017, n. 48370), si ritiene necessario un "correttivo" al dettato di cui all'art. 266 *bis* c.p.p., rimasto immune alla smania riformatrice dell'ultimo tempo, in modo da tipizzare l'uso del *Trojan* quale nuova tecnica di esecuzione delle captazioni di flussi di comunicazioni relativi a sistemi informatici o telematici.

Inoltre, a fronte delle molteplici funzionalità del captatore informatico e della legittimazione delle stesse da parte della giurisprudenza di legittimità, sarebbe auspicabile che il legislatore proceda con un intervento "additivo", atto a tipizzare le svariate attività di indagine derivanti dall'impiego del *malware* e che risultano diverse e/o aggiuntive rispetto alla mera intercettazione di conversazioni e comunicazioni tra presenti.

Si tratta di uno degli aspetti più delicati della materia, dal momento che l'esperimento delle attività di perquisizione occulta da remoto – mai disciplinata da alcuna norma giuridica – determina un *vulnus* ai principi fondanti l'assetto costituito, presidiati da norma costituzionali e convenzionali. In questi casi, il rischio da scongiurare è consentire alla prassi giurisprudenziale di ricorrere al concetto di "prova atipica" per giustificare e

legittimare il compimento di attività che, per converso, risultano ai limiti della costituzionalità.

Al fine di arginare simili *pericula*, si potrebbe propendere per l'introduzione di un nuovo mezzo di ricerca della prova per regolare le attività di osservazione e acquisizione di dati e informazioni da remoto mediante l'impiego di sempre più sofisticate tecniche di indagine. In particolare, appare doveroso individuare i "casi" e i "modi" di acquisizione di dati diversi dalle conversazioni comunicazioni e, di conseguenza, estranei alla disciplina delle intercettazioni *strictu sensu* intese. Con ciò non si intende "imbrigliare" in un eccessivo formalismo giuridico le attività di polizia ma solo rendere conforme ai principi propri di uno Stato di diritto un sistema che, ad oggi, è ancora orfano di regole (D. Curtotti, *Procedimento penale e* intelligence *in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Proc. pen. giust*., 2018, n. 3, p. 438).

Ma non basta. La necessità di un intervento riformatore in materia di investigazioni mediante agente intrusore è avvertita anche sul versante preventivo, soprattutto in rapporto alle altre forme di sorveglianza e controllo esperibili in fase procedimentale, sia in punto di previsione di specifici requisiti per il trattamento e l'utilizzo dei dati acquisiti, che di controllo in merito alla liceità e alla legittimità dell'attività condotta.

Non vanno, tuttavia, sottaciuti i rischi che possono derivare da un simile approccio "attivistico", fondato, cioè, sulla convinzione per cui la tipizzazione dei casi e di modi dell'intrusione informatica – sia in fase preventiva che repressiva – rappresenti la soluzione ai "mali" del sistema.

Come sempre accade quando il processo penale si confronta con i nuovi ritrovati della scienza e della tecnica, il pericolo è quello di intervenire su una materia già diventata obsoleta, perché - si sa – i tempi delle riforme non coincidono con la velocità propria del progresso e dell'evoluzione tecnologica, condannando la legge ad una obsolescenza *ab origine.*

Così, probabilmente, si potrebbe preferire una soluzione "più mite", sicuramente meno efficiente in punto di "certezza del diritto" ma altrettanto efficace in relazione alla protezione dei diritti fondamentali e, quindi, assolutamente corretta in un impianto garantista. Seguendo una simile impostazione, «il legislatore non dovrebbe soffermarsi sulla disciplina dei singoli strumenti informatici - sempre potenzialmente in evoluzione e dunque suscettibili di creare un vuoto di tutela in caso di mancato tempestivo intervento legislativo - ma dovrebbe piuttosto identificare le garanzie fondamentali che devono essere sempre tutelate indifferentemente dallo strumento impiegato» (C. Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *Dir. pen. cont.,* 1 giugno 2017).

Alla luce di tali considerazioni, si ritiene auspicabile un intervento legislativo atto ad identificare chiaramente non tanto tutte le singole tecnologie utilizzabili nel campo dell'intrusione informatica quanto piuttosto le garanzie fondamentali che devono essere sempre riconosciuti all'indagato, ai soggetti terzi occasionalmente coinvolti, nonché a coloro che risultano solo "attenzionati" nel corso delle investigazioni proattive, a prescindere dallo strumento impiegato.

La predisposizione di una norma "aperta", sulla falsariga del disposto di cui all'art. 189 c.p.p., che subordini strumenti di ricerca della prova a condizioni tassative, consente

di vincolare l'ingresso di nuove e sempre più evolute tecniche di indagine e di investigazione al rispetto delle garanzie fondamentali costituzionalmente riconosciute, in modo tale da ripristinare un sistema informato al principio di legalità della prova.

*****

A conclusione di questo percorso accademico stimolante ed avvincente, mi sia consentito ringraziare quanti hanno contribuito a trasformare una simile esperienza in un'occasione unica di crescita scientifica, professionale e, soprattutto, umana.

Innanzitutto, un grazie al Prof. Sergio Lorusso, ben più di un "semplice" tutor nel percorso dottorale, insostituibile mente a cui chiedere ausilio e consiglio.

Un profondo e sentito ringraziamento alla Prof.ssa Cinzia Motti, indispensabile punto fermo. Un grazie di cuore per avermi sostenuto e supportato nei momenti di difficoltà.

Intendo, inoltre, ringraziare il Prof. Vittorio Santoro e il Prof. Alessandro Palmieri, per cui nutro immensa stima e profonda gratitudine per gli stimoli intellettuali offerti in questo percorso.

Un grazie anche all'Università di Foggia, una grande famiglia che mi ha accolto con amore indimenticabile e, in particolare, a Gigi, un fratello "acquisito" che con pazienza e comprensione ha reso migliori le mie giornate. A Te, amico mio insostituibile, dieci, cento, mille volte grazie.

Last but not least, la Prof.ssa Donatella Curtotti, mio Maestro, guida, esempio. A Lei devo tutto. I nostri dialoghi, le riflessioni, le mille idee, la voglia di fare, costruire, pensare e proiettarsi al futuro, hanno reso questi anni meravigliosi. Un grazie infinito per esserci stata sempre, per aver creduto in me e avermi insegnato a muovere piccoli passi in questo strano e oscuro mondo.

*****