Percorso dottorale sviluppato con il sostegno finanziario di NextGenerationEU:
Missione 4, Componente 2, Investimento 3.3, CUP B63C22000990008
Borsa MUR- ex DM 352/2022 C.N.A. Servizi srl - Caf imprese

Dipartimento di Giurisprudenza

Dottorato in Scienze Giuridiche

38° Ciclo

Coordinatore: Prof. Alessandro Palmieri

Il rapporto tra titolare e responsabile del trattamento dei dati personali. Un'analisi del *Data Processing Agreement* alla luce dell'art. 28 GDPR

Settore scientifico disciplinare: Diritto Privato

Candidata
Roberta Nucciarone
Sede di attività
Università degli Studi di Siena

Firma digitale del/della candidato/a

Supervisore
Prof. Gabriele Salvi
Ente di appartenenza
Università degli Studi di Siena

Co-supervisore/i
Nome
Ente di appartenenza

Anno accademico di conseguimento del titolo di Dottore di ricerca
2025/2026

Università degli Studi di Siena
Dottorato in Scienze Giuridiche
38° Ciclo

Data dell'esame finale

_____

Commissione giudicatrice

_____
_____
_____
_____
_____

Supplenti

_____
_____

Indice

Introduzione……**7**

Capitolo I. Dalla Direttiva 95/46 CE al Regolamento UE 679/2016……**17**

1. La protezione dei dati nel continente europeo: il passaggio dalle normative nazionali alla Direttiva 95/46 CE…….17

1.1. Il fallimento della Direttiva 95/46 CE: un'analisi delle principali cause……..24

L'innovazione tecnologica…….. 24

La disomogeneità delle norme europee sulla protezione dei dati personali….25

2. Il GDPR e il rovesciamento di prospettiva rispetto alla Direttiva 95/46 CE..30

3. Gli attori del trattamento dei dati…….35

3.1. Il titolare del trattamento o *data controller*……..36

3.2. Il responsabile del trattamento o *data processor*……43

3.3. Il sub-responsabile del trattamento……..47

3.4. L'incaricato del trattamento…….49

4. Il principio di *accountability.* Una rivoluzione nella regolazione della *data protection*…… 50

4.1. La responsabilizzazione degli attori del trattamento fra Direttiva 95/46 CE e GDPR……..57

Capitolo II. La responsabilità da trattamento illecito dei dati personali……**59**

1. Il nuovo approccio del GDPR fra recessività dell'autodeterminazione e centralità del rischio……..59

1.1. Il *risked based approach* ……66

1.2. L'autoregolamentazione nel GDPR: numerosi gli strumenti contemplati dal Regolamento…….. 68

Le certificazioni…….. 69

I codici di condotta……71

1.2.1. Certificazioni e codici di condotta come "*Accountability Tools*"……. 74

2. Dalla responsabilizzazione alla responsabilità degli attori del trattamento…..75

2.1. La responsabilità *ex* art. 23 della Direttiva 95/46 CE e la sua attuazione nella legislazione italiana……76
2.1.1. Cenni sull'attuazione della responsabilità *ex* art. 23 della Direttiva 95/46 CE nelle legislazioni europee……82
3. La responsabilità *ex* art. 82 GDPR: gli elementi costitutivi della fattispecie…83
I danneggiati……83
I danneggianti…… 85
Il danno risarcibile……86
Il danno risarcibile nell'ordinamento giuridico italiano…… 88
3.1. La responsabilità per illecito trattamento dei dati. Una natura giuridica controversa……92
La responsabilità ex *art. 82 GDPR come responsabilità da inadempimento*..92
La responsabilità ex *art. 82 GDPR come responsabilità ancipite*……..94
La responsabilità ex *art. 82 GDPR come responsabilità extracontrattuale*..95
3.2. La responsabilità *ex* art. 82 GDPR, una responsabilità autonoma e speciale…97
3.2.1. Uno sguardo alla giurisprudenza europea sul danno immateriale……..98
La giurisprudenza tedesca…… 98
La giurisprudenza austriaca…….. 100
La giurisprudenza olandese……100
La giurisprudenza italiana……..101
Riflessioni conclusive sulla produzione giurisprudenziale europea……103
3.2.2. Le criticità della responsabilità *ex* art. 82 GDPR al vaglio della Corte di Giustizia: il caso UI contro *Österreichische Post AG*…….. .103
4. La responsabilità solidale degli attori del trattamento……106
4.1. Titolarità congiunta del trattamento e responsabilità solidale……107
4.2. I soggetti esonerati dal regime di responsabilità solidale……..110
Il sub-responsabile del trattamento……..110
Il Data Protection Officer……...112

Capitolo III. Il *Data Processing Agreement*: uno strumento chiave per la ripartizione delle responsabilità…… **115**
1. Il *Data Processing Agreement*……... 115
1.1. Il contratto di *outsourcing*: natura giuridica e diffusione……116

1.2. Il contratto di *outsourcing* nel trattamento dei dati. La suddivisione dei ruoli……...120
1.3. La designazione del *processor* prima e dopo il GDPR……..122
2. *Internet of Things*, un ambito complesso in cui il DPA assume una funzione cruciale……..123
2.1. La diffusione dei sistemi IoT nella società odierna……125
Energia……..125
Sanità……..125
Agricoltura…… 126
Edilizia……126
2.1.1. Le *Smart Homes*: un esempio emblematico dell'importanza del *Data Processing Agreement*…….127
2.2. Profili critici della negoziazione nell'universo IoT, e non solo……..131
2.2.1. Conformità del *Data Processing Agreement* al GDPR. La posizione dell'autorità svedese nel caso del Comune di Salem……132
2.3. Il *Cloud of Things*: una pluralità di contratti e di contraenti……...134
3. Il *Cloud Computing* e la distribuzione dei ruoli alla luce del GDPR……..139
3.1. *Cloud Consumer* e *Cloud Service Provider*, titolari o responsabili del trattamento?.....140
3.1.1. Il caso *Wirtschaftsakademie*……143
3.1.2. Dal caso *Wirtschaftsakademie* al caso *Fashion ID*: una lettura più restrittiva della contitolarità…… 146
3.2. La contitolarità nei termini di servizio dei *cloud service provider*…….148
3.3. La struttura dei contratti di *cloud computing*…… 150
3.3.1. Il *Data Processing Agreement* e il difficile adattamento al modello del *cloud computing*……... 151
4. Responsabilità e allocazione dei costi nel *Data Processing Agreement*…….153

Capitolo IV. La tutela dei dati personali in Croazia fra Direttiva 95/46 CE e GDPR. Un'analisi sulla regolazione del *Data Processing Agreement*…….157
1. La Direttiva 95/46 CE e la legge "ZZOP" del 2003……..157
2. La Croazia si conforma al GDPR: la "*Zakon o provedbi Opće uredbe o zastiti podataka"*……..161
2.1. L'adeguamento al GDPR, una sfida per le piccole e medie imprese croate..162

3. Il *Data Processing Agreement* e il modello elaborato dall'AZOP……..165
3.1. La responsabilità di *controller* e *processor*: modelli a confronto……..172
Le clausole contrattuali standard della Commissione Europea e il modello AZOP di Data Processing Agreement……..172
Le clausole contrattuali standard della Datatilsynet *e il modello AZOP di* Data Processing Agreement……...174
4. La responsabilità per illecito trattamento dei dati personali. Uno sguardo alla disciplina croata…….177

Bibliografia…… **181**

Giurisprudenza citata…… **198**

Decisioni citate di autorità amministrative indipendenti…… **201**

Introduzione

Con l'evoluzione tecnologica, si è assistito all'aumentare della circolazione dei dati personali. Dinanzi a tale fenomeno, è apparso fondamentale garantire una tutela efficace ai soggetti ai quali tali dati appartengono, ragion per cui ha trovato pieno riconoscimento il diritto alla privacy. Quest'ultimo, però, non è l'unico diritto avente ad oggetto i dati personali, dovendo a tal proposito menzionarsi anche il diritto alla protezione dei dati personali. Mentre il primo si è affermato come il diritto "ad essere lasciati soli", e quindi può essere fatto coincidere con il diritto alla riservatezza, il secondo è il diritto alla titolarità dei propri dati e alla tutela degli stessi. Ebbene, proprio da questo diritto prende le mosse il presente lavoro, che ripercorre l'evoluzione storica del diritto alla protezione dei dati, dalla sua comparsa nella *Hessische Datenschutzgesetz,* la legge federale dell'Assia del 1970, fino alla sua prima regolazione a livello europeo, con la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, nota come Convenzione 108. Malgrado gli sforzi dei legislatori nazionali, molti dei quali tentarono di riprodurre i principi della Convenzione nelle normative interne, la protezione dei dati personali in Europa rimaneva frammentata e disomogenea. Per colmare tali discrepanze, fu adottata la Direttiva 95/46 CE, che, tuttavia, dovendo essere recepita dai singoli Stati Membri, si rivelò ben presto inidonea ad assicurare eguali livelli di tutela ai dati personali.

L'inadeguatezza della Direttiva non passò inosservata, né alla Commissione Europea, che avviò una procedura di consultazione pubblica al fine di revisionarla, né agli attori coinvolti nel processo, tra i quali il Garante europeo per la protezione dei dati, che invitò ad utilizzare un diverso strumento giuridico per disciplinare la materia. Sulla scia di tali rilievi, nel 2016 fu adottato il Regolamento Generale sulla Protezione dei Dati Personali, o GDPR *(General Data Protection Regulation*). Il Regolamento, benché non abbia totalmente ovviato all'assenza di armonizzazione, come dimostrano le oltre sessanta clausole di apertura in esso contenute, ha senz'altro garantito un livello di protezione più omogeneo ai dati personali. In questa prospettiva, il GDPR ha ribaltato l'impostazione della normativa previgente: mentre la Direttiva poneva al centro l'interessato (*data subject*), e i diritti di cui egli

godeva in relazione ai propri dati, il GDPR ha spostato l'attenzione sugli altri soggetti che intervengono nel trattamento dei dati, specialmente sul titolare (*data controller*) e sul responsabile (*data processor*). Solo attraverso un rafforzamento degli oneri e delle responsabilità di questi ultimi, infatti, può essere assicurata una tutela effettiva dei diritti dell'interessato.

Passando ad esaminare il concetto di trattamento dei dati, si osserva come questo sia contraddistinto dalla tensione fra il *data subject*, da un lato, e il *controller* e il *processor*, dall'altro, i quali dispongono dei dati dell'interessato per finalità predeterminate dal titolare. La definizione degli scopi del *data processing*, insieme alla scelta dei mezzi da impiegare, è ciò che caratterizza la figura del *controller*, rendendolo un elemento imprescindibile: non può esservi un trattamento di dati personali senza un soggetto che ne assuma la titolarità. Tale qualifica può derivare da fonti legali, negoziali o da prassi, ma deve comunque trovare riscontro nella realtà fattuale. Infatti, al di là della classificazione formale, il *controller* è colui che detiene, in concreto, il potere decisionale sulle finalità del trattamento. Emblematico, in tal senso, è il caso SWIFT, che ha evidenziato come, anche in assenza di un rapporto contrattuale, un soggetto possa essere considerato un titolare laddove abbia effettivamente determinato lo scopo del trattamento. Diversamente dal *controller,* il *processor* non è una figura necessaria, ma facoltativa. Invero, il responsabile ha un ruolo strumentale rispetto a quello del titolare: se quest'ultimo stabilisce le finalità, il responsabile si limita ad eseguire il trattamento secondo le istruzioni ricevute. Tuttavia, qualora il *processor* concorra alla definizione degli scopi, esso assume la veste di titolare, o contitolare, del trattamento.

Alle figure appena menzionate il GDPR ha riservato particolare attenzione, pur non essendo queste le uniche disciplinate al suo interno; al contrario, il Regolamento ha introdotto delle disposizioni sul sub-responsabile del trattamento, totalmente privo di regolazione nella Direttiva 95/46 CE. Un'altra rilevante novità prevista dal GDPR è rappresentata dal principio di *accountability*, anch'esso assente nella precedente Direttiva. Se quest'ultima si limitava ad imporre al titolare l'onere di garantire il rispetto dei principi fondamentali del trattamento, il Regolamento ha trasformato tale obbligo in una piena responsabilizzazione. Il *controller*, infatti, non solo deve conformarsi alle disposizioni del Regolamento, ma deve anche essere in grado di dimostrarlo. Il principio in esame, benché formalmente enunciato all'art. 24 GDPR, permea l'intero impianto normativo e

costituisce il fondamento di numerosi obblighi sanciti dal Regolamento, come la tenuta del registro delle attività di trattamento.

Se è vero che il GDPR ha consolidato il ruolo del titolare del trattamento, è altresì vero che ha operato modifiche ancor più significative sulla figura del responsabile. Mentre la Direttiva imponeva al *processor* esclusivamente di eseguire le istruzioni del *controller*, il GDPR grava il responsabile di molteplici obblighi, oltre a riconoscerne la responsabilità per i danni derivanti da eventuali trattamenti illeciti dei dati. Ne deriva una maturazione concettuale del *processor,* che cessa di essere un soggetto passivo e assume una posizione attiva nel garantire il rispetto della normativa.

L'insieme degli aspetti sopracitati, ovvero l'inasprimento degli obblighi del *controller*, l'introduzione di nuovi oneri e responsabilità per il *processor*, nonché la regolazione di figure ausiliarie come il sub-responsabile, costituisce il mezzo attraverso cui il GDPR persegue il suo obiettivo principale: la responsabilizzazione di tutti gli attori del trattamento dei dati personali. Alla base di un simile intento, vi è la concezione del legislatore europeo, poc'anzi anticipata, secondo cui la piena tutela dei dati personali non può essere raggiunta con il mero riconoscimento di facoltà in capo all'interessato, poiché quest'ultimo non sempre è in grado di esercitarle consapevolmente. In quest'ottica, il GDPR impone obblighi al responsabile e amplia il novero di oneri a carico del titolare, al quale richiede di adottare misure preventive, quali la valutazione di impatto e la nomina di un *Data Protection Officer* (DPO). Queste misure sono state ideate dal legislatore europeo per responsabilizzare il *controller* e, allo stesso tempo, eliminare, o quantomeno ridurre, i rischi connessi alla gestione dei dati personali. Il GDPR, infatti, abbandona un approccio di tutela *ex post* in favore di uno preventivo, orientato a evitare i danni sin dall'origine. Al centro della nuova impostazione vi sono l'analisi e la gestione del rischio, insieme alla responsabilizzazione del titolare, elementi che promuovono una tutela dei dati più efficace. Tale concezione si concretizza nel cosiddetto "approccio basato sul rischio" (*risk-based approach*), che obbliga i *controller* ad adottare misure appropriate per garantire la sicurezza dei dati, in funzione della natura e della gravità dei rischi legati ai trattamenti effettuati. La connessione tra il *risked based approach* e il principio di *accountability* è ulteriormente rafforzata dall'autoregolamentazione privata. Quest'ultima, oltre a permettere una maggiore flessibilità nella gestione del rischio, facilita la

dimostrazione di conformità da parte degli attori del trattamento grazie agli "*accountability tools*", come codici di condotta e certificazioni. Sebbene l'adesione a tali strumenti non sia di per sé sufficiente a garantire la *compliance*, il GDPR riconosce che, in molte circostanze, l'uso dei *tools* costituisce una prova del rispetto del principio di *accountability*, inteso come la capacità di dimostrare la conformità al Regolamento.

Il principio di *accountability* non ha inciso solo sul versante degli obblighi, ma ha avuto un impatto anche sulla responsabilità civile per il trattamento illecito dei dati. In particolare, ha influito sulla legittimazione passiva e sull'onere probatorio, andando a delineare una forma di responsabilità diversa rispetto a quella della Direttiva 95/46 CE. L'art. 23 della Direttiva stabiliva che chiunque fosse danneggiato da un trattamento illecito avesse diritto ad essere risarcito dal titolare, il quale poteva esonerarsi dimostrando che il danno non gli era in alcun modo imputabile. Il legislatore aveva quindi definito un modello di responsabilità presunta, con una prova liberatoria basata sul caso fortuito, che doveva essere recepito nelle normative nazionali. In Italia, l'art. 23 è stato inizialmente trasposto nell' art. 18 della legge 31 dicembre 1996, n. 675, e successivamente attuato dall'art. 15 Codice della Privacy. Tale articolo ha rappresentato, per il nostro ordinamento, la tipizzazione dell'illecito civile conseguente al trattamento dei dati personali, nonché l'introduzione di una nuova fattispecie di responsabilità oggettiva.

Tuttavia, gli Stati Membri non sono riusciti a recepire l'art. 23 della Direttiva in maniera uniforme, discostandosi gli uni gli altri su quali condotte integrassero un trattamento illecito, come pure sulla risarcibilità o meno dei danni non patrimoniali. In un panorama legislativo così disgregato, si avvertiva l'esigenza di un sistema omogeneo di regole in materia di responsabilità, esigenza che ha trovato compimento nell'art. 82 del Regolamento. La norma stabilisce che <<chiunque subisca un danno>> derivante da un trattamento illecito dei dati, possa essere risarcito. L'espressione <<chiunque>> ha sollevato diversi dubbi interpretativi, potendo essere intesa sia in senso estensivo, e quindi ricomprendere tutti i danneggiati, indipendentemente dal loro status di interessato, sia in senso restrittivo, riferendo la potestà risarcitoria solo al *data subject*. Per quanto riguarda l'individuazione dei responsabili, l'art. 82 prevede che il *controller* e il *processor* siano entrambi tenuti a rispondere del danno, da intendersi in senso ampio. La norma, infatti, consente il risarcimento tanto dei pregiudizi materiali, quanto di

quelli immateriali, al fine di garantire una compensazione effettiva per il *data subject*. Nonostante ciò, le corti nazionali si sono mostrate caute nell'accogliere le richieste risarcitorie di danni immateriali, esigendo prove concrete di pregiudizi specifici. Le principali problematiche connesse al risarcimento dei danni immateriali sono essenzialmente due: la difficoltà di dimostrarli, trattandosi di lesioni che incidono sulla sfera personale dell'individuo, e la complessità della loro quantificazione. L'art. 82 del GDPR, del resto, non prevede un criterio standardizzato per determinare l'entità del danno, rimettendo tale valutazione alla discrezionalità delle corti nazionali. In questo contesto, caratterizzato da interpretazioni divergenti, un punto di svolta è rappresentato dalla sentenza della Corte di Giustizia dell'Unione Europea nel caso *UI contro Österreichische Post AG*. In tale pronuncia, i giudici di Lussemburgo hanno chiarito che la nozione di "danno immateriale" deve essere intesa in modo autonomo e uniforme a livello europeo, senza rinviare alle discipline nazionali. Secondo la Corte, questa interpretazione è coerente con l'obiettivo del GDPR di garantire un livello omogeneo di tutela in tutta l'Unione. Nonostante l'indubbia rilevanza della decisione, essa presenta alcune criticità che verranno approfondite nel corso della trattazione.

Il danno immateriale non rappresenta l'unico profilo problematico dell'art. 82 GDPR. Al contrario, la norma presenta diverse lacune, che hanno reso necessario l'intervento dei legislatori nazionali, i quali hanno dovuto ricostruire gli aspetti mancanti alla luce dei rispettivi regimi di responsabilità. In Italia, ciò ha dato origine a un dibattito sulla qualificazione dell'art. 82 GDPR; nello specifico, ci si chiede se debba essere ricondotto alla responsabilità extracontrattuale, come stabilito dal previgente art. 15 Codice della Privacy, o se debba piuttosto essere considerato una fattispecie di responsabilità da inadempimento, o ancora una forma di responsabilità ancipite. Certo è che l'art. 82 GDPR disciplina un'ipotesi di responsabilità solidale tra tutti coloro che partecipano al trattamento lesivo dei dati. In questo contesto, titolari, contitolari e responsabili del trattamento sono congiuntamente responsabili nei confronti dell'interessato, mentre la norma non fa riferimento né al sub-responsabile né al DPO. Inoltre, l'art. 82 GDPR stabilisce che, nei rapporti interni, debba essere valutato il contributo causale di ciascun soggetto, in modo che chi abbia risarcito l'intero danno possa rivalersi sugli altri titolari e/o responsabili.

In uno scenario come quello appena descritto, in cui una pluralità di attori intervengono nel medesimo trattamento dei dati con funzioni e responsabilità differenti, non poteva non assumere un ruolo cruciale l'atto che disciplina le relazioni tra di essi, specialmente quella tra *controller* e *processor*. Già la Direttiva 95/46 CE prevedeva che il titolare designasse un responsabile tramite un atto giuridico o un contratto, senza tuttavia regolarne in modo dettagliato i requisiti sostanziali. Il Regolamento, invece, all'art. 28, introduce un vero e proprio *Data Processing Agreement* (DPA), che rappresenta il fulcro dell'analisi condotta nel presente lavoro. Sebbene il legislatore europeo abbia stabilito una serie di requisiti, sia sostanziali che formali, a cui il *controller* deve attenersi qualora affidi il trattamento a un soggetto terzo (il *processor*), non è riuscito a evitare che tali accordi venissero utilizzati a vantaggio della parte contrattualmente più forte. Quest'ultima, contrariamente a quanto si potrebbe ritenere, non coincide sempre con il titolare del trattamento. Al contrario, un'analisi approfondita di ambiti specifici, quali l'*Internet of Things* e il *cloud computing*, o della loro integrazione nel cosiddetto *Cloud of Things*, rivela come spesso sia proprio il responsabile a dettare le condizioni del *Data Processing Agreement.* In questi settori si configura una dinamica ben diversa rispetto a quella delineata nel Regolamento, il quale presuppone che, laddove un soggetto esternalizzi parte della sua attività, incluso il trattamento dei dati ad essa connesso, per concentrare le risorse sul proprio *core business*, sia il *controller* a disporre di maggior potere negoziale. D'altronde, tale soggetto è titolare sia dell'attività economica principale, che del trattamento dei dati personali. Tuttavia, quello che la normativa europea non considera, è che chi viene incaricato del trattamento non agisce come responsabile per un unico cliente, ma per diversi, stipulando con ciascuno specifici contratti di *outsourcing.* Questa molteplicità di rapporti conferisce al *processor* una posizione negoziale di forza, che si traduce nella redazione unilaterale dei *Data Processing Agreement*, sottoposti ai titolari per l'accettazione, senza reali margini di revisione o negoziazione. Ciò si verifica tanto nell'ambito dell'*Internet of Things*, quanto in quelli ad esso strettamente collegati, come il *cloud computing*. Un caso esemplificativo è quello di Google che, in qualità di fornitore di servizi *cloud,* tratta dati personali per conto di una vasta platea di clienti, dai quali riceve istruzioni formali in merito alle operazioni da svolgere. Benché, in apparenza, siano i clienti a dettare le istruzioni per il trattamento, la realtà è ben diversa, poiché è il fornitore del servizio

(*processor*) a predisporre condizioni standardizzate, spesso non negoziabili, imponendo ai clienti (*controller*) una scelta tra accettazione integrale o rinuncia al servizio. Tale formulazione contrattuale rende estremamente complessa, se non impossibile, una rinegoziazione da parte dei titolari, i quali si trovano a dover accettare clausole sbilanciate.

Uno degli aspetti più critici nella redazione dei *Data Processing Agreement* è rappresentato dalle disposizioni sulla responsabilità derivante dal trattamento illecito dei dati. Invero, molti fornitori di servizi adottano clausole contrattuali che mirano a circoscrivere la propria responsabilità, disponendo che le conseguenze dei propri illeciti ricadano sul cliente. A tali previsioni, si affianca un'altra strategia adoperata dai *service provider* che agiscono in qualità di *processor*: fissare un tetto massimo al risarcimento a cui possono essere chiamati. Tale soglia è solitamente fatta coincidere con l'ammontare delle commissioni corrisposte dal cliente nei mesi precedenti. Una simile somma, però, risulta insufficiente rispetto all'entità dei danni che il titolare potrebbe subire a causa di una violazione dei dati da parte del responsabile. Del resto, oltre alle sanzioni amministrative comminate dalle autorità di controllo, il *controller* potrebbe dover affrontare gravosi oneri economici, ai quali potrebbero aggiungersi i danni reputazionali.

Un'iniqua ripartizione della responsabilità non è l'unica criticità che emerge dall'applicazione pratica del *Data Processing Agreement* di cui all'art. 28 GDPR. Il Regolamento, infatti, non contempla una disciplina esplicita sull'allocazione dei costi tra titolare e responsabile, lasciando questo aspetto alla libera negoziazione delle parti. In linea di principio, qualora i costi derivino da una condotta del *provider*, quest'ultimo dovrebbe farsi carico delle spese connesse all'adempimento degli obblighi normativi e dei provvedimenti delle autorità competenti, nonché di tutte le azioni necessarie a ripristinare i diritti lesi dell'interessato. Tuttavia, sempre più spesso si assiste a una prassi opposta, secondo cui è il titolare del trattamento a dover sostenere i costi legati agli audit e alle verifiche di conformità. Ancora una volta, la discrezionalità concessa alle parti nella redazione del *Data Processing Agreement* viene sfruttata dal contraente forte a proprio vantaggio.

Se fino a questo momento sono state sottolineate le mancanze del Regolamento, occorre riconoscere al legislatore europeo il merito di aver fornito strumenti di supporto a titolari e responsabili del trattamento, attribuendo alla Commissione Europea, come pure alle autorità di controllo nazionali, il potere di

adottare clausole contrattuali standard (SCCs) da utilizzare nei *Data Processing Agreement.* Analizzando esempi concreti dell'esercizio di tale facoltà, ci si soffermerà sul complesso di SCCs elaborate dalla Commissione Europea. Le clausole costituiscono un modello contrattuale conforme al GDPR, che gli attori del trattamento possono adoperare per garantire legittimità alle proprie operazioni. Sebbene non sia obbligatoria, l'adozione delle SCCs è comunque auspicabile, in quanto la loro totale inclusione negli accordi assicura la piena conformità al Regolamento. Diversamente, l'inserimento parziale delle clausole, o la loro modifica, può compromettere la *compliance*. È indubbio che le SCCs costituiscano un valido strumento per coloro che faticano ad adeguarsi al GDPR; eppure, queste non sono esenti da criticità, non riuscendo a colmare tutte le lacune del GDPR. Tra gli aspetti più problematici, non adeguatamente disciplinati dalla Commissione, figura quello della responsabilità delle parti. Difatti, la Decisione di esecuzione (UE) 2021/914 con la quale sono state adottate le SCCs non dedica un articolo specifico al tema, limitandosi a menzionarlo nell'allegato relativo alle misure tecniche e organizzative. Un simile vuoto regolatorio evidenzia un limite strutturale delle clausole contrattuali standard, che demandano alle parti aspetti essenziali della disciplina, esponendole a potenziali squilibri contrattuali.

Tra gli interventi nazionali, si distingue il modello danese, che rappresenta un riferimento importante per l'adeguamento al GDPR. L'Autorità per la protezione dei dati locale, riscontrando difficoltà nella redazione di *Data Processing Agreement* che ottemperassero al GDPR, ha elaborato un set di SCCs, sottoponendolo al Comitato europeo per la protezione dei dati (EDPB). Dopo una prima valutazione dell'EDPB, e successive modifiche, l'Autorità danese ha finalizzato delle SCCs che, pur non essendo obbligatorie, offrono vantaggi concreti: l'adozione integrale delle clausole, purché riprodotte fedelmente, esclude controlli dell'autorità nazionale. L'EDPB ha formulato osservazioni dettagliate sul contenuto delle SCCs, richiedendo, ad esempio, una descrizione precisa delle misure tecniche e organizzative. Tuttavia, sull'aspetto cruciale della responsabilità, il Comitato si è limitato a delle considerazioni generali, senza esigere modifiche alla Clausola 13. Quest'ultima consente alle parti di definire liberamente gli aspetti non trattati dalle SCCs, inclusa la responsabilità, ma senza stabilire condizioni specifiche o fornire criteri interpretativi. Tale superficialità contrasta con l'approccio dettagliato seguito per altre clausole, lasciando alle parti la possibilità

di inserire disposizioni sfavorevoli per il contraente debole. Un approccio leggermente diverso è stato adottato dall'autorità croata, la quale ha predisposto un modello contrattuale nazionale che, seppur non qualificabile come SCCs, è senz'altro utile per gli attori del trattamento locali. Allo stesso modo, quest'intervento appare rilevante per il tema oggetto del presente lavoro. Invero, l'Autorità croata ha riconosciuto che il *Data Processing Agreement* costituisce un mezzo per conformarsi al GDPR, sollecitandone l'adozione. A differenza del modello danese, quello croato dedica un paragrafo specifico alla responsabilità, tracciando indicazioni che, per quanto sommarie, guidano le parti nella redazione dell'accordo. Pertanto, esso rappresenta un tentativo più coerente di affrontare un aspetto centrale che, altrimenti, rischierebbe di non essere adeguatamente disciplinato.

Alla luce di quanto brevemente anticipato, e che sarà oggetto di approfondimento nel prosieguo della trattazione, non può non riconoscersi l'importanza del GDPR nell'aver introdotto l'obbligo di stipulare un *Data Processing Agreement*, fissando un quadro normativo di riferimento per la regolazione dei rapporti tra titolare e responsabile del trattamento. Tuttavia, appare altrettanto evidente che la formulazione dell'art. 28 GDPR, insieme all'assenza di SCCs realmente esaustive, ha generato incertezze e disomogeneità applicative. Da un lato, le autorità nazionali, pur proponendo modelli utili, non sono riuscite a colmare del tutto le lacune del Regolamento. Dall'altro, la Commissione Europea ha optato per un approccio eccessivamente cauto su temi delicati come la responsabilità da trattamento illecito dei dati. Per assicurare una tutela effettiva delle parti coinvolte, e garantire un'applicazione uniforme del GDPR, è necessario un intervento più decisivo: la Commissione Europea, o in alternativa un numero significativo di autorità di controllo nazionali, dovrebbe elaborare nuove clausole contrattuali standard che regolino in modo puntuale i profili ancora irrisolti, a partire dalla responsabilità di cui all'art. 82 GDPR. Quanto a quest'ultima, le clausole dovrebbero includere definizioni chiare, criteri oggettivi per l'attribuzione della responsabilità, nonché indicazioni sulla prova liberatoria. Solo così sarà possibile evitare che la libertà contrattuale si traduca in un indebolimento delle tutele previste dalla normativa sulla protezione dei dati personali, con il rischio che i *Data Processing Agreement*, da strumenti di garanzia, si trasformino in fonti di pericolo per gli attori più vulnerabili. D'altronde, l'esperienza applicativa ha

evidenziato come i margini di discrezionalità lasciati dal legislatore abbiano spesso favorito il contraente più forte, compromettendo l'equilibrio auspicato. L'esempio dei fornitori di servizi *cloud* e dell'*Internet of Things* è emblematico: la loro capacità di imporre condizioni standardizzate e non negoziabili svuota di significato il principio di responsabilizzazione reciproca, rendendo illusoria l'effettività delle garanzie per il titolare del trattamento.

In definitiva, la diffusione di nuove clausole contrattuali standard appare la via più efficace per assicurare alle parti coinvolte nel trattamento una tutela piena ed effettiva, a condizione che la responsabilità, finora relegata a un generico richiamo normativo, venga disciplinata in maniera dettagliata al loro interno.

Capitolo I

Dalla Direttiva 95/46 CE al Regolamento UE 679/2016

Sommario: 1. La protezione dei dati nel continente europeo: il passaggio dalle normative nazionali alla Direttiva 95/46 CE; 1.1. Il fallimento della Direttiva 95/46 CE: un'analisi delle principali cause; 2. Il GDPR e il rovesciamento di prospettiva rispetto alla Direttiva 95/46 CE; 3. Gli attori del trattamento dei dati; 3.1. Il titolare del trattamento o *data controller*; 3.2. Il responsabile del trattamento o *data processor*; 3.3 Il sub-responsabile del trattamento; 3.4. L'incaricato del trattamento; 4. Il principio di *accountability.* Una rivoluzione nella regolazione della *data protection; 4.1.* La responsabilizzazione degli attori del trattamento fra Direttiva 95/46 CE e GDPR

1. La protezione dei dati nel continente europeo: il passaggio dalle normative nazionali alla Direttiva 95/46 CE

Il 24 maggio del 2016 ha rappresentato uno snodo fondamentale per la protezione dei dati personali: è entrato in vigore il Regolamento Generale sulla Protezione dei Dati Personali, o GDPR *(General Data Protection Regulation*), il quale, a due anni da tale data, ha trovato effettiva applicazione nei 27 Stati membri dell'Unione Europea, nonché nel Regno Unito. Il Regolamento, tuttavia, si è inserito all'interno di un panorama normativo già esistente, come chiarito dallo stesso all' art. 94, ove si afferma che <<la Direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018>>.

Benché il sistema a pilastri dell'Unione Europea ne avesse limitato l'area di applicazione, la Direttiva 95/46 CE, sino a quel momento, aveva rappresentato il principale strumento dell'Unione per la protezione dei dati[1]. Essa, infatti, incorporava i principi fondamentali in materia di dati personali, costituendo la

[1] Per ulteriori precisazioni sull'ambito di applicazione della Direttiva 95/46 CE, v. B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione Europea*, 2013, n. 2, p. 319, il quale chiarisce che <<la Direttiva 95/46 non si applica ad attività come quelle previste dall'allora titolo VI del trattato sull'Unione europea, né, in ogni caso, ai trattamenti relativi alla pubblica sicurezza, alla difesa, alla sicurezza dello Stato o alle attività dello Stato in materia di diritto penale>>.

disciplina di riferimento sia per la normativa intra-UE[2], che per altri testi di vario *status* giuridico nazionali ed internazionali[3].

I principi confluiti nella Direttiva 95/46 CE erano il frutto di un lungo percorso evolutivo che aveva avuto origine molto prima della sua introduzione. Invero, il diritto alla privacy era stato riconosciuto quale diritto fondamentale già al termine della Seconda Guerra Mondiale: in seguito alla costituzione, nel 1949, del Consiglio d'Europa. Quest'ultimo era volto a promuovere i diritti umani nell'intero continente europeo, ragion per cui, ad appena un anno dalla sua istituzione, redasse e adottò la Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU). Ebbene, nella CEDU il diritto alla privacy veniva tutelato nella forma del diritto al rispetto della vita privata[4] e gli si attribuiva una dignità pari a quella delle consolidate libertà di religione ed espressione, enunciate agli articoli successivi. Tuttavia, malgrado il diritto alla privacy avesse ottenuto pieno riconoscimento nella CEDU, la tutela effettivamente garantitagli si rivelò insufficiente dinanzi al "boom" tecnologico che caratterizzò gli anni Sessanta. Difatti, i rapidi progressi nel campo dell'elaborazione elettronica dei dati, unitamente alla comparsa dei computer *mainframe*[5], avevano permesso alle amministrazioni pubbliche e alle grandi imprese di creare ampie banche dati, oltre che di migliorare e incrementare la raccolta, l'elaborazione e l'interconnessione dei dati personali. Simile sviluppo, da un lato, aveva comportato notevoli vantaggi in termini di efficienza e produttività, dall'altro, aveva però rivelato una tendenza all'archiviazione elettronica massiva di dati relativi alla sfera privata degli individui. Dinanzi a questo fenomeno, il Consiglio d'Europa non poté che stabilire un quadro di principi e norme specifiche al fine di prevenire la raccolta e il trattamento illecito dei dati personali[6]. A tale risultato, si giunse grazie all' intervento dell'Assemblea

---

[2]A titolo esemplificativo: la Direttiva 2002/58 CE (Direttiva ePrivacy) del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; la Decisione quadro 2008/997/GAI del Consiglio del 27 novembre 2008, riguardante la protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia.

[3] Si fa riferimento, in particolare, alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, unitamente al suo Protocollo Aggiuntivo.

[4] Il diritto alla privacy è tutelato ai sensi dell'art. 8, par. 1, CEDU, il quale, già nella versione del 1950, disponeva <<*everyone has the right to respect for his private and family life, his home and his correspondence*>>.

[5] I *mainframe* sono computer ad alte prestazioni con grandi quantità di memoria e processori che elaborano in tempo reale miliardi di semplici calcoli e transazioni.

[6]Sull'esigenza di pervenire ad un sistema normativo unitario per contrastare la raccolta illecita di dati, v. Consiglio d'Europa, *Human Rights and Rule of Law, Data Protection, Background,* disponibile *online* su www.coe.int/t/dghl/standardsetting/dataprotection/History.

Parlamentare del Consiglio d'Europa; quest'ultima, infatti, rivolse al Comitato dei Ministri una raccomandazione[7] affinché verificasse che la CEDU ed il diritto interno degli Stati membri fossero in grado di tutelare il diritto alla privacy rispetto alle moderne tecnologie. In risposta, fu condotto uno studio, su incarico del Comitato dei Ministri, il quale svelò l'inadeguatezza delle legislazioni nazionali in materia[8]. Alla luce di ciò, lo stesso Comitato intervenne adottando diverse risoluzioni, nonché definendo principi e linee guida per la standardizzazione della protezione dei dati personali tra i Paesi membri del Consiglio d'Europa[9].

In seguito, tali principi confluirono nelle legislazioni nazionali europee; invero, già nel 1970 lo Stato federale dell'Assia adottò la prima legge sulla protezione dei dati, la *Hessische Datenschutzgesetz*. Oltre al primato cronologico, alla disciplina in esame è altresì attribuibile il merito di aver introdotto il termine "*datenschutz*", vale a dire l'espressione *data protection*, o protezione dei dati personali, la quale ha poi integrato il diritto internazionale ed il diritto dell'Unione Europea, oltre che gli ordinamenti giuridici dei vari Stati membri. Al termine "*datenschutz*" la legge dell'Assia attribuiva un duplice significato: diritto ad ottenere, trasmettere e conservare i dati ottenuti da elaborazioni automatizzate; facoltà di escluderne la consultazione, alterazione, o distruzione da parte di soggetti non autorizzati. Dunque, la *Hessische Datenschutzgesetz* recepiva il bisogno collettivo di riservatezza, concependo la protezione dei dati come diritto alla salvaguardia degli stessi mediante l'adozione di misure proibitive. Il trattamento dei dati finiva così per essere un'eccezione, in quanto la regola era che i dati non dovevano essere trattati[10].

---

[7]Crf. la Raccomandazione dell'Assemblea Parlamentare (68)509 del 31 gennaio 1968 relativa alla necessità di tutela dei diritti umani e, in particolare, del diritto alla privacy. A tal proposito, l'Assemblea evidenzia come i moderni sviluppi tecnologici, quale l'intercettazione telefonica e simili, rappresentino una minaccia nei confronti del diritto alla privacy, soprattutto a fronte di legislazioni nazionali inadeguate.

[8] Cfr. Consiglio d'Europa, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* in *European Treaty Series*, n. 108, ove si osserva che, laddove l'elaborazione automatica dei dati personali coinvolga parti di diversi Paesi, potrebbe non essere facile determinare quale Stato abbia giurisdizione e quale legge nazionale si applichi. Pertanto, in materia, sarebbe auspicabile promuovere la cooperazione internazionale, unico strumento utile alla risoluzione di tali problematiche.

[9] Tra le principali risoluzioni si possono segnalare: risoluzione del Comitato dei Ministri (73)22 del 26 settembre 1973, la quale ha stabilito il principio della protezione dei dati per il settore privato; risoluzione del Comitato dei Ministri 74(29) del 20 settembre 1974 che ha enunciato il medesimo principio rispetto al settore pubblico.

[10] Cfr. H. Burkert, *Privacy - Data Protection. A German/European Perspective*, in C. Engel, K.H. Keller (a cura di), *Governance of Global Networks in the Light of Differing Local Values,* Baden Baden, Nomos Verlagsgesellschaft, 2000, pp. 43 e ss.

Fuori dal continente europeo, invece, fu adottato un approccio differente: negli Stati Uniti, infatti, al concetto di *data protection* veniva contrapposto quello di privacy. Quest'ultima, secondo Westin[11], era da intendersi come il diritto di individui, gruppi, o istituzioni, di determinare da sé quando, come, e in che misura, le informazioni che li riguardavano potessero essere comunicate ad altri. Siffatta concezione si discostava ampiamente dal modello federale tedesco, giacché riconosceva ai titolari dei dati non solo il diritto a negare il trattamento, bensì una serie di prerogative positive.

Lo Stato federale tedesco, tuttavia, non fu l'unico all'interno dell'Unione ad accogliere la nozione di *data protection*; eclatante fu il caso svedese, in quanto fu il primo Paese al mondo ad adottare, nel 1973, una regolazione omnicomprensiva sulla protezione dei dati, valevole per ogni situazione[12]. A pochi anni di distanza, nel 1978, anche l'Austria adottò la legge federale sulla protezione dei dati, la *Datenschutzgesetz*, la quale attribuiva al diritto alla *data protection* rango costituzionale. Nel medesimo anno, la Francia emanò la *Loi Informatique et Libertés*, che, in parte discostandosi dagli altri esempi europei, si soffermava sull'attività del trattamento dei dati; infatti, la legge presupponeva che questi dovessero essere trattati, pertanto ne regolava le condizioni[13].

Nonostante gli Stati membri avessero recepito i principi enunciati dalle risoluzioni del Consiglio d'Europa, già durante la fase preparatoria di detti testi era emerso come la protezione dei dati personali non potesse prescindere da norme internazionali vincolanti. D'altro canto, il medesimo suggerimento era stato avanzato dalla Conferenza dei Ministri della Giustizia europei, ove si era affrontato il tema dei pericoli derivanti da un uso sregolato delle banche dati elettroniche. In merito, si era osservato che, pur potendo invocare alcune disposizioni di diritto civile e penale, gli individui avrebbero ottenuto maggiore protezione contro la conservazione illecita dei loro dati mediante una convenzione internazionale[14].

Suddetta convenzione fu adottata solo nel 1981, quando, al termine di quattro anni di negoziati, il Consiglio d'Europa presentò la Convenzione sulla

---

[11] A.F. Westin, *Privacy and Freedom,* New York, Atheneum, 1967, pp. 7 e ss.
[12] Cfr. R. Pagano, *Informatica e diritto*, Milano, Giuffrè, 1986, pp. 74 e ss.
[13] Per una panoramica sulle discipline di protezione dei dati personali in ambito europeo, v. G. Gonzalez Fuster, S. Gutwirth, *Opening up personal data protection: a conceptual controversy*, in *Computer Law & Security Review*, vol. XXIX, 2013, n. 5, pp. 531 e ss.
[14] Settima Conferenza dei Ministri della Giustizia europei tenutasi a Basilea dal 15 al 18 maggio 1972.

protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, anche nota come Convenzione 108. Quest'ultima, rivestì un ruolo fondamentale nella regolamentazione della raccolta di dati personali, nonché nella protezione da abusi o usi impropri di tali dati, giacché era, ed è tuttora, l'unico strumento internazionale giuridicamente vincolante nel campo della protezione dei dati[15]. Sottoscrivendo la Convenzione 108, gli Stati membri[16] si sono impegnati ad adottare le misure necessarie per proteggere i dati e per dare attuazione ai principi della Convenzione nel proprio diritto interno. Quanto a tale aspetto, affinché i principi possano dirsi integrati nella legislazione nazionale, occorre che la stessa preveda: la raccolta equa e lecita dei dati, il trattamento e l'archiviazione dei dati per finalità legittime, il divieto di servirsi dei dati per scopi incompatibili con tali fini e di conservarli più a lungo del necessario. Inoltre, la Convenzione stabilisce la libera circolazione dei dati personali tra gli Stati aderenti; tuttavia, essa impone delle restrizioni ai flussi laddove il Paese destinatario non fornisca una protezione equivalente a quella sancita dalla Convenzione. Infine, compiendo un altro passo avanti nella tutela dei dati personali, la Convenzione 108 conferisce ad ognuno il diritto di conoscere quando siano state memorizzate informazioni sul proprio conto e, se necessario, di farle correggere[17].

Sebbene gran parte degli ordinamenti europei si fosse dotato di normative attuative della Convenzione, particolarmente interessante il *Data Protection Act* inglese del 1984[18], in altre esperienze, invece, perdurava una situazione di vuoto regolatorio che dottrina e giurisprudenza stentavano a colmare. Tale era il caso dell'Italia, dove alla sottoscrizione della Convenzione 108 erano seguite delle proposte di legge, nonché la presentazione di un disegno di legge, nessuna delle quali si era mai concretizzata. Invero, nel 1986 suddetto disegno, presentato il 4 maggio 1984, era ancora sotto l'esame della Commissione giustizia, senza che fosse

[15] Sulla portata della Convenzione 108 sul diritto alla protezione dei dati nel panorama europeo, v. Consiglio d'Europa, *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni dell'Unione europea, 2018, pp. 27 e ss.

[16] La Convenzione adottata a Strasburgo il 28 gennaio 1981 è stata attualmente ratificata da cinquantacinque Stati, tra i quali rientrano tutti i quarantasei Stati membri del Consiglio d'Europa.

[17] Per un'analisi approfondita del testo della Convenzione, v. C. Glon, *Data Protection in the European Union: A Closer Look at the Current Patchwork of Data Protection Laws and the Proposed Reform That Could Replace Them All*, in *International Journal of Legal Information*, vol. XLII, 2014, n. 3, pp. 473 e ss.

[18] Circa l'esempio virtuoso di attuazione inglese della Convenzione, v. F.G.B. Aldhouse, *U.K. Data Protection – Where are we in 1991?*, in *Yearbook of Law Computers and Technology*, 1991, n. 5, pp. 180 e ss.

stato avviato l'*iter* parlamentare; stessa sorte, d'altronde, era toccata alle proposte normative[19].

In un simile contesto, quindi, caratterizzato dalla disomogeneità nella protezione dei dati personali, si colloca l'intervento armonizzatore europeo, ossia la Direttiva 95/46 CE. Quest'ultima ha rappresentato un punto di svolta nella tutela dei dati personali, poiché ha apportato delle innovazioni significative in materia. Prima fra tutte, quella di aver introdotto principi e strumenti volti a ridurre la posizione di asimmetria informativa tra titolare del trattamento e persona interessata. Al centro della disciplina, infatti, ha posto il consenso dell'interessato, il quale doveva essere libero, informato e inequivocabilmente prestato. A tal scopo, la Direttiva richiedeva che il consenso fosse preceduto da un'informativa sufficientemente dettagliata, *in primis*, sull'entità dei dati e le loro modalità di conservazione, *in secundis*, sulle finalità della raccolta e l'eventuale trasmissione a terzi. Da siffatto principio, la normativa europea ha fatto quindi derivare: da un lato, i diritti dell'interessato, tra cui il diritto all'informazione in tutte le fasi del trattamento stesso, il diritto alla revoca del consenso e quello alla cancellazione dei dati ceduti; dall'altro, i corrispondenti obblighi gravanti sul titolare del trattamento[20].

Oltre alla riduzione dell'asimmetria informativa, e dunque all'introduzione del principio del consenso, alla Direttiva si riconosce di aver elaborato altri principi volti a limitare la raccolta dei dati personali, imponendo l'obbligo di trattare i soli dati necessari ad adempiere alle finalità prestabilite. In tale prospettiva, una delle norme più lungimiranti della Direttiva era quella dove si stabiliva che <<gli Stati membri riconoscono ad ogni persona il diritto a non essere sottoposta ad una decisione che produca effetti giuridici o che abbia effetti significativi nei suoi confronti, fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento e così via>>[21].

Ebbene, pur avendo la Direttiva 95/46 CE provveduto a ridefinire i principi della Convenzione 108, e benché questi abbiano trovato ulteriore attuazione nella

---

[19] R. Pagano, *Informatica e diritto*, cit., pp. 87 e ss.
[20] Cfr. M.G. Stanzione, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto privato*, 2016, n. 4, pp. 1249 e ss.
[21] Ciò, è espressamente previsto ai sensi dell'art. 15 della Direttiva 46/95 CE, adottata dal Parlamento europeo e dal Consiglio europeo il 24 ottobre 1995.

legislazione europea[22], il Trattato di Lisbona ha reso evidenti le carenze del citato sistema. Quest'ultimo, infatti, ha posto una notevole enfasi sulla protezione dei diritti fondamentali, specialmente sul diritto alla protezione dei dati. Ciò, si evince sia dalla Carta fondamentale dei diritti dell'Unione Europea, a cui il Trattato ha riconosciuto la stessa efficacia giuridica dei trattati, poiché essa annovera la protezione dei dati personali tra i diritti fondamentali[23]; sia dall'art. 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE), al quale il Trattato di Lisbona ha fatto coincidere la nuova base giuridica per la protezione dei dati. Quest'ultima è applicabile ai trattamenti di dati personali tanto nel settore pubblico, quanto in quello privato, ivi compresi gli ambiti della cooperazione giudiziaria e di polizia, della politica estera e di sicurezza comune. Così facendo, il Trattato di Lisbona ha adottato un nuovo approccio orizzontale, teso ad eliminare le divergenze che ostacolano una protezione omogenea, coerente ed efficace dei dati personali di tutti gli individui[24]. Viene, dunque, ribaltata la concezione del previgente art. 286 del TCE, emendato dal Trattato di Lisbona, il quale imponeva un obbligo di tutela solo a istituzioni e organismi comunitari, lasciando che fossero gli atti derivati a disporre una tutela di carattere generale[25]. Al contrario, nella nuova impostazione si ammette che la tutela di tale diritto abbia portata *erga omnes*, in quanto non possono sottrarsi ad un simile dovere né soggetti investiti di pubbliche funzioni, sia europei che nazionali, né, tanto meno, soggetti privati.

---

[22] Nel panorama legislativo europeo in materia di protezione di dati emergevano: il Regolamento (CE) n. 45/2001, applicabile al trattamento dei dati da parte delle istituzioni e degli organismi dell'UE; la Direttiva 2002/58/CE sulla privacy e le comunicazioni elettroniche (Direttiva ePrivacy); la decisione quadro 2008/977/GAI sulla protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale.

[23] L'art. 8 della Carta dei diritti fondamentali dell'Unione Europea (CDFUE o Carta di Nizza), adottata a Nizza il 7 dicembre 2000, al primo paragrafo stabilisce che <<ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano>>.

[24]Così l'art. 16 TFUE, come modificato dal Trattato di Lisbona, ricalca quanto previsto dall'art.8 del CDFUE nella misura in cui riconosce che <<ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano>>.

[25] Cfr. B. Cortese, *Commento all'art. 286 TCE,* in A. Tizzano (a cura di), *Trattati dell'Unione e della Comunità Europea*, Milano, Giuffrè, 2004, pp. 1284 e ss.

1.1. Il fallimento della Direttiva 95/46 CE: un'analisi delle principali cause

L'innovazione tecnologica

In un simile contesto, la Direttiva 95/46 CE dovrebbe rappresentare il mezzo per garantire una tutela effettiva dei dati personali a livello globale. Difatti, questo obbiettivo appare raggiungibile solo riaffermando le nozioni chiave in essa contenute, nonché i suoi principi. In particolare, dovrebbero ritrovare vigore i principi di: legittimità, equità, proporzionalità, limitazione delle finalità e della trasparenza; unitamente ai diritti dell'interessato ed al controllo indipendente da parte delle autorità pubbliche[26].

Tuttavia, la Direttiva, lungi dall'assumere tale ruolo, ha rivelato la sua inidoneità a ricoprirlo a fronte dell'innovazione tecnologica che ha seguito la sua adozione. D'altronde, questa era stata concepita in un panorama informatico nettamente diverso; pertanto, mal si adattava alle nuove tecnologie ed all' impatto che queste avevano avuto sui processi aziendali e sulle attività governative. Infatti, la transizione digitale aveva dato vita a modelli e strumenti capaci di influenzare il funzionamento di tutti servizi e, di rimando, la vita delle persone. Alla luce di ciò, la Direttiva, benché ideata come tecnologicamente neutrale ed applicabile in ogni settore, rischiava di essere scardinata dalla nuova generazione di tecnologie e, a sua volta, dalla nuova generazione di utenti[27]. Negli ultimi anni, del resto, non era solo la tecnologia ad essere cambiata, bensì coloro che la utilizzavano: la cd. "*Bit Generation*"[28]. Quest'ultima era, ed è tutt'ora, composta da persone che condividevano informazioni personali *online*, comunicavano con i propri conoscenti mediante i *social network* e riuscivano per sino a "trasmettere" la propria posizione, in tempo reale, attraverso i *digital devices*. Si assiste, dunque, ad un

[26]Gruppo di lavoro per la protezione dei dati personali (Art. 29), Gruppo sulle attività di polizia e giustizia (WPPJ), *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP 168), 1 dicembre 2009, par. 2.16, disponibile *online* su https://ec.europa.eu/justice/article-29.

[27]Cfr. O. Tene, *Privacy: The new generations*, in *International Data Privacy Law*, vol. I, 2011, n.1, pp. 15 e ss.

[28] L'espressione "*Bit Generation*" è usata per riferirsi ai <<giovani nati tra gli anni Ottanta e Novanta e cresciuti nel flusso digitale, nel passaggio dalle tecnologie analogiche a quelle digitali>>, così L. Savonardo, *Pop music, media e culture giovanili: dalla* Beat Revolution *alla* Bit Generation, in *Convergenze culturali*, Milano, EGEA, 2017, p.110.

cambiamento nelle modalità di interazione tale per cui la sfera privata si confonde sempre di più con quella pubblica[29].

Dinanzi a suddetta transizione, gli enti governativi di tutto il mondo, tra cui la Commissione Europea[30] e l'OCSE[31], non hanno potuto ignorare che ad una nuova generazione di tecnologie, così come di utenti, non poteva non corrispondere un eguale rinnovamento nella *governance* della protezione dei dati.

La disomogeneità delle norme europee sulla protezione dei dati personali

Ad ogni modo, l'inadeguatezza rispetto alla recente innovazione tecnologica non era stato l'unico limite della Direttiva 95/46 CE; infatti, malgrado il testo fosse stato introdotto per colmare il divario tra legislazioni nazionali che, dalla fine degli anni Ottanta, ostacolava la libera circolazione dei dati nel mercato interno, non si ottenne l'effetto di armonizzazione desiderato.

Analizzando più nel dettaglio la situazione dei vari Paesi, si evince come la Direttiva sia stata recepita in tempi piuttosto rapidi dalla maggior parte dei legislatori europei. In Spagna, ad esempio, il testo ha trovato attuazione già nel 1999 all'interno della *Ley Organica n. 15 de Protección de Datos de Carácter Personal* (LOPD), la quale è entrata in vigore il 14 gennaio 2000[32]. Menzione a parte merita la Germania che, come anticipato, fin dagli anni Settanta si era dotata di un'ampia disciplina in materia di dati personali, sia a livello federale che nei *Länder*[33]. Difatti, ognuno dei sedici *Länder* aveva adottato la propria normativa in materia e ne garantiva l'osservanza tramite la autorità di protezione dei dati locale. A livello

---

[29] Sulla commistione fra sfera pubblica e privata, v. M. Belluati, *Reti, spazi e culture. Verso nuovi orizzonti pubblici*, in F. Corbisiero, E. Ruspini (a cura di), *Sociologia del futuro. Studiare la società del ventunesimo secolo,* Padova, Cedam, 2016, pp.82 e ss.

[30] In merito alla posizione assunta dalla Commissione Europea, v. ACCIS, *Position Paper on the Consultation on the legal framework for the fundamental right to protection of personal data,* dicembre 2009, pp. 3 e ss, disponibile *online* su https://homeaffairs.ec.europa.eu/document/download/7d7387285a7d4b61b2329aa3a1747152_en?filename=accis_en.pdf&prefLang=cs.

[31]Organizzazione per la cooperazione e lo sviluppo economico (OCSE, in inglese OECD), *The OECD Privacy Framework*, 2013, pp. 3 e ss., disponibile *online* su https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[32] La *Ley Organica n. 15 de Protección de Datos de Carácter Personal* (LOPD) è stata approvata dal Parlamento il 13 dicembre 1999. Sulla portata e il significato della normativa, v. A. Troncoso Reigada, *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Cívitas, 2010.

[33] I *Länder*, o Stati federati, sono le sedici entità politiche e amministrative che insieme formano la Repubblica Federale di Germania.

federale, invece, il Parlamento aveva, dapprima, emanato il *Bundesdatenschtuzgesetz*, o BDSG, del 1977 ed, in un secondo momento, la legge del 1990 e il BDSG del 2001, così da dare operatività alla Direttiva. Lo scopo generale di tale quadro normativo era proteggere l'individuo contro le violazioni dei suoi diritti personali, i "*personlichkeitsrecht*", attraverso il trattamento dei dati personali[34]. Posizione a sé stante occupa anche il Regno Unito, che si è conformato al regime di protezione dei dati della Direttiva a decorrere dal 1 marzo 2000, sostituendo il già esistente *Data Protection Act* del 1984 con il *Data Protection Act* del 1998. Quanto alla Francia, è stata l'ultimo Paese a dare attuazione alla Direttiva 95/46 CE mediante la legge del 6 agosto 2004, la quale ha modificato la previgente *Loi Informatique e Libertés* del 1978[35]. Venendo, infine, all'ordinamento italiano, il processo di recepimento della Direttiva ha avuto inizio con l'introduzione della legge 31 dicembre 1996, n. 675, a cui è poi seguito un percorso di razionalizzazione conclusosi con l'entrata in vigore del Codice in materia di protezione dei dati personali[36]. In tal modo, veniva fatta confluire in un unico testo una regolamentazione che si era stratificata nel tempo, a causa di numerosi interventi modificativi e integrativi[37].

Malgrado l'accoglimento generalizzato della Direttiva, non possono non evidenziarsi, però, le divergenze attuative che emergono già in relazione ai primi articoli della stessa[38]. Infatti, la natura e lo *status* della protezione dei dati varia

---

[34] Cfr. D. Banisar, S. Davies, *Global trends in privacy protection: an international survey of privacy, data protection, and surveillance laws and development*, in *John Marshall Journal of Computer & Information Law*, vol. XVIII, 1999, n.1, pp. 44 e ss.

[35] Per una panoramica completa del quadro storico sulle discipline di protezione dei dati personali in ambito internazionale ed europeo, v. G. Buttarelli, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676*, Milano, Giuffrè, 1997, pp.71 e ss. Più di recente, in sintesi, v. *Privacy: Profili di diritto comparato*, ottobre 2018, disponibile *online* su https://www.diritto.it/privacy-profili-diritto-comparato/.

[36] Il Codice in materia di protezione dei dati personali, o Codice della privacy, è stato approvato con il d.lgs. 30 giugno 2003, n. 196, ed è entrato in vigore il 1° gennaio 2004. Successivamente, con la piena attuazione del GDPR, il Codice ha subito un processo di modifica ad opera del d.lgs. 10 agosto 2018, n. 101.

[37] Così il Garante per la protezione dei dati personali, *Stato di attuazione del Codice in materia di protezione dei dati personali - Relazione 2004 - 9 febbraio 2005*, par. 1.1., disponibile *online* su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1093797, il quale osserva che <<la nuova disciplina ha provveduto a semplificare alcuni adempimenti e ad attribuire un ruolo significativo, anche in una prospettiva di deflazione legislativa, ai codici di deontologia e di buona condotta, soggetti alla preventiva verifica da parte del Garante>>.

[38] In particolare, notevoli discrepanze affiorano già in relazione all'art. 1, par. 1, della Direttiva 95/46/CE, ove si enuncia che <<gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali>>.

ampiamente da uno Stato all'altro. Alcuni Paesi, fra cui la Spagna, contemplano espressamente la *data protection* in Costituzione mediante specifiche disposizioni; queste ultime, richiamando il contenuto dell'art. 8 della Carta di Nizza, regolano la protezione dei dati come un diritto *sui generis*. Ciò nonostante, nelle loro leggi, o nella loro giurisprudenza, tali Stati tendono comunque a ricollegare la *data protection* ad altri diritti generali o specifici, quale il diritto alla privacy (Portogallo); il diritto alla vita privata e all'onore (Spagna); o ancora al diritto generale al rispetto della propria "personalità" (Paesi Bassi). Allo stesso modo, l'Austria, che ha attribuito rango di diritto costituzionale alla protezione dei dati sin dal 1978, lo tutela nella forma del diritto alla riservatezza, oltre che come diritto alla vita privata. Diversamente, in altri Paesi la protezione dei dati non viene esplicitamente menzionata in Costituzione, ma deriva da principi costituzionali generali o specifici. Così in Germania, ove la protezione dei dati, pur avendo un elevato *status* costituzionale, non viene enunciata in modo esplicito dalla Carta fondamentale, bensì proviene dal diritto generale al rispetto della personalità: <<*das allgemeine Persönlichkeitsrecht*>>[39]. Parimenti, in Francia la *data protection* trae fondamento da disposizioni costituzionali enuncianti altri diritti, quali il rispetto dell'identità umana e della vita privata, nonché delle libertà individuali e pubbliche. Altri Paesi, fra cui l'Italia, collegano la protezione dei dati al diritto alla privacy*,* costituzionalmente tutelato[40]. Caso a sé stante è poi quello del Regno Unito, il quale, non avendo una Costituzione scritta, inizialmente non garantiva alla protezione dei dati alcun *status* speciale; tuttavia, quando il Paese ha

[39] Tale diritto, infatti, è espressamente previsto dalla Legge fondamentale della Repubblica federale della Germania, la quale, all'art. 2, riconosce in capo ad ogni individuo il diritto al libero sviluppo della propria personalità.

[40] La Costituzione italiana non fa espresso riferimento al diritto alla privacy; tuttavia, essa ne garantisce la tutela mediante un insieme di norme volte a proteggere il singolo nella sua vita privata. Fra queste, di particolare rilievo è l'art. 2, ai sensi del quale <<la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale>>. La disposizione in esame rappresenta il fulcro del principio personalista, in quanto riconosce i diritti inviolabili dell'uomo non solo in relazione alla sfera sociale, ma anche a quella individuale. In virtù di ciò, l'art. 2 della Costituzione rappresenta lo spunto per riconoscere la privacy quale valore costituzionalmente protetto (v. Corte costituzionale – Servizio Studi, *Tutela della vita privata: realtà e prospettive costituzionali. Quaderno predisposto in occasione dell'incontro trilaterale delle Corti costituzionali spagnola, portoghese e italiana*, Lisbona, 1- 4 ottobre 2006, pp. 7 e ss.). Fra le norme a tutela della vita privata si pone, fra le altre, anche l'art. 12 della Costituzione, il quale stabilisce che <<nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni>>.

recepito la Convenzione europea dei diritti dell'uomo, ha finito per conferirle uno *status* rafforzato. Invero, nella misura in cui si può affermare che la *data protection* deriva da diritti sanciti dalla Convenzione, quale, ad esempio, il diritto alla vita privata e familiare, si riconosce a quest'ultima una protezione rafforzata[41].

Difficoltà concernenti un'armonizzazione omogenea si notano altresì in relazione al recepimento delle definizioni che la Direttiva fornisce all'art. 2. Se è vero, infatti, che gli Stati hanno attribuito ai concetti base (dati personali, trattamento, consenso) un significato quasi del tutto analogo a quello della normativa europea, è pur vero che talvolta vi hanno apportato delle modifiche "minori", tali da determinare risultati differenti[42]. Pertanto, a causa di dette variazioni minime, certi dati saranno considerati "personali" in alcuni Paesi, ma non in altri; alcuni sistemi di archiviazione saranno considerati sufficientemente strutturati secondo una data legge nazionale, ma insufficientemente articolati, o non facilmente consultabili, per un'altra.

La medesima problematica si riscontra in merito ai principi enunciati dalla Direttiva 95/46 CE e trasfusi nelle legislazioni europee. Esemplificativo, in questo senso, è il principio di specificazione e limitazione delle finalità, il quale è stabilito con termini identici, o molto simili, a quelli utilizzati dalla Direttiva dalla maggior parte degli Stati membri. Nonostante la similarità, la vaghezza stessa del principio lascia però aperta la possibilità di applicazioni divergenti, ragion per cui gli Stati si servono di test per verificare l'incompatibilità del trattamento. Tuttavia, tali test variano a seconda del Paese: alcuni adottano il test delle "ragionevoli aspettative" dell'interessato (Belgio); altri, quello del bilanciamento (Germania e Paesi Bassi); altri ancora collegano la verifica al rispetto dei principi di salvaguardia, trasparenza, legalità ed equità (Regno Unito e Grecia)[43].

Alla luce di questi ultimi rilievi, la Direttiva del 1995, benché incorporasse al suo interno obbiettivi e principi ancora validi, appariva ormai come una

---

[41] In questo senso, v. D. Korff, *Report on the findings of the study*, in *EC Study on implementation of data protection directive*, n.3, 2002, pp.12 e ss.

[42]Sulle sfide di armonizzazione poste dalla Direttiva, in special modo dalle definizioni di cui all'art. 2, v. Commissione Europea – Direzione Generale per la Giustizia, Libertà e Sicurezza, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, gennaio 2010, pp. 28 e ss., disponibile *online* su https://op.europa.eu/en/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b.

[43] Per una panoramica dei diversi test di incompatibilità del trattamento, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Opinion 03/2013 on purpose limitation* (WP 203), 2 aprile 2013, par.2.1, disponibile *online* su https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

regolamentazione inidonea. Pertanto, emergeva la necessità di un quadro normativo che fosse più solido e coerente, tale da adeguarsi allo sviluppo dell'economia digitale nel mercato interno[44]. Al raggiungimento di tale obbiettivo contribuì senza dubbio il Trattato di Lisbona, il quale aveva abolito il sistema dei pilastri, nonché riconosciuto il diritto alla protezione dei dati quale diritto autonomo rispetto alla privacy. Si presentava, allora, l'opportunità di sfruttare il nuovo *status* giuridico acquisito per rielaborare il modello di protezione dei dati dell'Unione Europea e colmare le lacune del passato.

L'auspicato processo di modifica della Direttiva ebbe iniziò nel 2009, quando la Commissione Europea diede avvio ad una consultazione pubblica che culminò nella pubblicazione di una comunicazione[45]. Successivamente, tutti i principali partecipanti al processo (il Consiglio Europeo, il Parlamento Europeo, il GEPD e il Gruppo di lavoro "Articolo 29"[46]) resero le loro opinioni sia sulla comunicazione della Commissione, sia sui possibili emendamenti della Direttiva. Di particolare interesse appare l'opinione del Garante europeo per la protezione dei dati (GEPD), l'unico ad aver ravvisato, nel processo di revisione in atto, l'occasione per riconsiderare il tipo di strumento giuridico per la protezione dei dati. Difatti, a parere del Garante, il Regolamento, in quanto direttamente applicabile negli Stati membri, sarebbe stato il mezzo più idoneo a garantire il diritto fondamentale alla protezione dei dati. Inoltre, questo avrebbe consentito la creazione di un mercato interno dove i dati personali avrebbero potuto circolare liberamente, godendo di un eguale livello di tutela, indipendentemente dal Paese di elaborazione. Il Regolamento avrebbe altresì ridotto lo spazio per interpretazioni contraddittorie e per divergenze ingiustificate nell'applicazione della legge. In ultimo, l'adozione di tale strumento avrebbe posto fine ad una delle questioni più controverse della Direttiva 95/46 CE: individuare la normativa applicabile alle operazioni di

[44]Cfr. E. Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori,* in *Contratto e Impresa*, 2018, n. 1, pp. 106 e ss.
[45]Cfr. Commissione Europea, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni "Un approccio globale alla protezione dei dati personali nell'Unione Europea",* COM (2010) 609, 4 novembre 2010, par.1, disponibile *online* su https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52010DC0609.
[46]Il Gruppo di Lavoro "Articolo 29" era un organismo consultivo indipendente istituito dalla Direttiva 95/46 CE, il quale si componeva di un rappresentante delle varie autorità nazionali, del Garante europeo della protezione dei dati e di un rappresentante della Commissione. L'obiettivo del Gruppo era garantire regole comuni in materia di privacy, adottando linee guida e pareri esplicativi della normativa vigente.

trattamento in corso nell'Unione Europea[47]. Ad eguali conclusioni, del resto, giunse la Commissione Europea, la quale già nella sua comunicazione aveva segnalato le difficoltà scaturenti dalla carenza di armonizzazione in materia di protezione dei dati. Infatti, la Commissione, in quella sede, aveva chiarito come la frammentazione delle legislazioni affliggesse sia i titolari del trattamento, chiamati ad affrontare il problema dell'incertezza giuridica relativa al trasferimento dei dati tra Stati; sia gli interessati, i quali rischiavano di vedere compromesso il livello di tutela uniforme che la Direttiva avrebbe dovuto garantire loro[48]. Pertanto, la Commissione suggerì l'adozione di un regolamento, piuttosto che una nuova direttiva, ritenendolo lo strumento più adatto a risolvere i problemi di armonizzazione tra gli Stati membri[49].

2. Il GDPR e il rovesciamento di prospettiva rispetto alla Direttiva 95/46 CE

Ebbene, sulla scia di tali considerazioni, nell'aprile del 2016 l'Unione Europea ha adottato il GDPR, il quale non rappresenta affatto <<*the end of the road, but a beginning of a new chapter*>>[50], come ha affermato la Commissaria Jourová nel suo discorso programmatico alla conferenza sul Regolamento Generale sulla Protezione dei Dati. Quest'ultimo, infatti, non solo consolida la *data protection* quale diritto fondamentale nel panorama giuridico successivo al Trattato di Lisbona, ma persegue altresì una duplice ambizione: garantire un elevato livello di tutela al diritto alla protezione dei dati personali; rimuovere ogni ostacolo alla circolazione dei dati[51].

---

[47] Garante europeo per la protezione dei dati, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, 14 gennaio 2011, par. 5.5, disponibile *online* su https://www.edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en.

[48]Cfr. Commissione Europea, *Comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni "Un approccio globale alla protezione dei dati personali nell'Unione Europea",* cit., par. 2.2.

[49]Commissione Europea, *Proposta di regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)*, COM/2012/011 final, 25 gennaio 2012, par. 11, disponibile *online* su https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=COM:2012:0011:FIN.

[50] Commissione Europea, *Commissioner Jourová speech at the General Data Protection Regulation conference,* 25 maggio 2018, p. 1, disponibile *online* su https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3949

[51] In questi termini, l'art. 1, parr. 2 e 3, del GDPR, secondo il quale il Regolamento <<protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati

Il GDPR ha dunque rappresentato uno spartiacque nel modo di intendere la protezione dei dati, giacché ha istituito un vero e proprio "modello europeo" in materia, basato su tre elementi principali. In primo luogo, il modello dell'Unione Europea attribuisce agli individui diritti che assicurano il controllo dei propri dati. Invero, questi hanno diritto a che i loro dati personali siano raccolti in modo equo e lecito, nonché per scopi legittimi, specifici ed espliciti. Quanto alla raccolta dei dati, essa deve altresì avvenire sulla base di un consenso libero, specifico e informato, oppure in virtù di un'altra base legittima. Inoltre, il GDPR stabilisce il diritto alla portabilità dei dati, il diritto alla cancellazione degli stessi ed il diritto all'oblio, i quali si aggiungono al novero dei diritti già stabiliti in materia, ossia il diritto di accesso, quello di opposizione e quello di rettifica. In secondo luogo, il modello in esame ha come fondamento la regolazione della protezione dei dati da parte del titolare e del responsabile del trattamento, sotto la supervisione delle autorità nazionali per la protezione dei dati (DPA). A queste ultime, il GDPR affianca un nuovo organismo europeo indipendente: il Comitato europeo per la protezione dei dati (EDPB), composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante della protezione dei dati delle istituzioni dell'Unione Europea (EDPS). Le DPA, insieme all'EDPB, devono agevolare la conformità delle parti al GDPR attraverso l'emanazione di linee guida e certificazioni, unitamente alla promozione di codici di condotta. In terzo luogo, il modello europeo, tramite il GDPR, prevede misure di attuazione più efficaci. Infatti, il Comitato europeo può adottare decisioni vincolanti quando diversi Paesi dell'Unione Europea siano coinvolti nello stesso caso. Oltre a ciò, le autorità nazionali di protezione dei dati sono dotate di poteri omogenei, fra i quali indispensabile è quello di infliggere multe alle imprese fino a venti milioni di euro, oppure fino al 4% del fatturato totale mondiale annuo di un'azienda. Infine, gli Stati hanno facoltà di introdurre rimedi, anche di natura giudiziaria, per far fronte a violazioni o danni causati dal mancato rispetto del GDPR[52].

Quanto agli aspetti formali, il GDPR è un regolamento "speciale" poiché contiene più di sessantanove clausole "di apertura", ragion per cui si è iniziato a

---

personali. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali>>.

[52] Circa il nuovo modello europeo di *data protection* istituito dal GDPR, v. O. Tambou, *Opening Remarks*, in K. Mc Cullagh et al. (a cura di), *National Adaptations of the GDPR,* Lussemburgo,, Collection Open Access Book, 2019, pp. 24 e ss.

dubitare della sua efficacia armonizzatrice. Con il termine armonizzazione, nel contesto europeo, ci si riferisce al processo di inserimento di un concetto negli ordinamenti giuridici nazionali, volto alla formazione di una nozione uniforme che sia funzionale agli obiettivi dell'Unione[53]. Le differenze giuridiche tra gli ordinamenti vengono quindi ad essere eliminate, o quanto meno attenuate, tramite il riavvicinamento delle leggi. Tuttavia, l'uso di clausole "di apertura" all'interno di misure di armonizzazione influisce in modo significativo sul livello di omogeneità delle stesse. Infatti, tali clausole si caratterizzano per la necessità di un'ulteriore concretizzazione; in particolare, quelle contenute negli strumenti di diritto derivato prescrivono, in linea di principio, deroghe obbligatorie per gli Stati membri, determinando così un'intensa interazione, ma allo stesso tempo concorrenza, fra il diritto dell'Unione Europea e quello nazionale[54]. In sostanza, a seconda del loro contenuto, le clausole "di apertura" possono avere un impatto più o meno forte sul riavvicinamento delle legislazioni nazionali, rafforzando o indebolendo la natura giuridica della misura di armonizzazione scelta.

Nell'ambito del GDPR sono state individuate molteplici clausole "di apertura", alcune obbligatorie: quale l'art. 51 del GDPR, in base al quale ogni Stato Membro deve introdurre norme per istituire un'autorità di controllo; altre facoltative: esemplificativo, in tal senso, è l'art. 8 del GDPR, il quale consente agli Stati di derogare al limite di sedici anni prescritto per il consenso del minore, purché non sia stabilita un'età inferiore a tredici anni. Considerata la vastità di clausole di questo tipo che ricorrono nel Regolamento, parte della dottrina ha rilevato come il GDPR sia formalmente un regolamento, ma nella sostanza una direttiva. Inoltre, la stessa dottrina ha altresì sostenuto che dette clausole favoriscono la creazione di ulteriori differenze fra le legislazioni nazionali, andando così a contrastare con l'obiettivo di armonizzazione che il Regolamento si pone[55].

---

[53] Per una puntuale specificazione della definizione di armonizzazione, v. E. Lohse, *The Meaning of Harmonisation in the Context of European Union Law – a Process in Need of Definition*, in M. Andenas, C. Andersen Baasch (a cura di), *Theory and Practice of Harmonisation*, Cheltenham, Edward Elgar Publishing, 2012, p. 28.

[54] Per una riflessione sul ruolo delle "clausole di apertura" nella legislazione europea, v. M. Muller, *Die Öffnungsklauseln der Datenschutzgrundverordnung: Ein Beitrag zur Europäischen Handlungsformenlehre*, Münster, Wissenschaftliche Schriften der WWU, 2018, pp. 175 e ss, il quale sottolinea come le clausole di apertura poste all'interno dei provvedimenti secondari aprano la via al diritto nazionale, stabilendo un obbligo di attuazione per gli Stati membri.

[55] Per tutti, v. E. Miscenic, A.L. Hoffmann, *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR),* in *EU and Comparative Law Issues and Challenges series,* 2020, n. 4, pp. 52 e ss.

Benché abbia fissato uno standard europeo di protezione dei dati, quindi, il GDPR presenta dei limiti evidenti, alcuni dei quali imputabili alla complessità del periodo in cui lo stesso è stato elaborato. Invero, il Regolamento ha visto la luce in un contesto storico caratterizzato, da una parte, dall' inasprimento dei rapporti fra gli operatori del settore digitale ed i gestori delle comunicazioni elettroniche; dall'altra, dall'aumento delle ostilità fra due delle più grandi potenze mondiali, ossia l'Europa e gli Stati Uniti. Queste ultime erano da ricondursi a quanto stabilito dalla pronuncia *Schrems*[56] in merito al significato dell'espressione <<livello di protezione adeguato>>[57]. Difatti, la Direttiva 95/46 CE ammetteva il trasferimento di dati personali dall'Unione Europea a Paesi terzi a condizione che lo Stato destinatario offrisse loro una tutela adeguata; tuttavia, non recava alcuna definizione del criterio, limitandosi ad asserire che l'adeguatezza dovesse essere valutata in relazione a <<tutte le circostanze relative al trasferimento>>[58]. A fronte di simili incertezze, la Corte di Giustizia dell'Unione Europea (CGUE) ha preliminarmente chiarito come la Direttiva debba essere interpretata alla luce dei diritti fondamentali stabiliti dalla Carta di Nizza, con particolare attenzione al diritto alla vita privata e alla protezione dei dati personali. Pertanto, affinché il livello di protezione possa dirsi adeguato, occorre che il Paese terzo garantisca una tutela dei diritti pari a quella offerta dalla Direttiva, interpretata secondo la Carta dei diritti fondamentali dell'Unione Europea. La CGUE, in tal modo, ha fornito un'interpretazione estensiva, se non manipolativa, del criterio di adeguatezza[59], fino a farlo coincidere con quello di sostanziale equivalenza della protezione[60]. Suddette valutazioni, d'altronde, non potevano non incidere sulla decisione con la quale la

---

[56] Corte di Giustizia dell'Unione Europea, 6 ottobre 2015, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, disponibile *online* su www.curia.europa.it.

[57] Il concetto di "livello di protezione adeguato" è richiamato dall'art. 25, par. 1, della Direttiva 95/46 CE, ove si afferma che <<gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali […] può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato>>.

[58] L'art. 25, par. 2, della Direttiva 95/46 CE prevede che <<l'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati>>.

[59] Il compito di valutare l'adeguatezza del livello di protezione è affidato, ai sensi dell'art. 25, par. 6, della Direttiva, alla Commissione Europea. Laddove quest'ultima rilevi l'inadeguatezza del livello di tutela assicurato da un Paese terzo, occorre che gli Stati membri adottino le misure necessarie a evitare qualsivoglia trasferimento di dati personali verso detto Paese.

[60] Sul punto, cfr. O. Pollicino, M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, in *Diritto dell'informazione e dell'informatica*, vol. XXXI, 2015, n. 4-5, pp. 77 e ss, i quali sostengono che la "trasfigurazione" del contenuto del test di legittimità, evidente in diversi passaggi della sentenza, sia giustificata dalla volontà di offrire un'interpretazione rinnovata dei diritti fondamentali alla privacy e alla tutela dei dati personali.

Commissione aveva riconosciuto l'adeguatezza del sistema "*Safe Harbor*"[61], invalidandola. L'invalidazione della piattaforma ha, inevitabilmente, generato disappunto nella classe industriale americana, la quale ha avvertito la pronuncia *Schrems* come un'interferenza in questioni di diritto interno; ma, soprattutto, ha prodotto nuova instabilità nei rapporti fra Unione Europea e Stati Uniti, essendo questi stati privati della piattaforma per il trasferimento dei dati[62].

Ebbene, rappresentando il prodotto della difficile epoca appena descritta, il GDPR non poteva non presentare carenze sotto una pluralità di aspetti. In aggiunta alla dibattuta questione dell'armonizzazione, infatti, è emerso come il Regolamento abbia adottato una sistematica poco chiara, la quale ha impedito al testo di fornire un quadro armonioso della tutela dei dati. Su questo piano, ad esempio, stupisce l'ampiezza del Capitolo III, il quale, articolato in cinque sezioni differenti, racchiude gran parte delle innovazioni del GDPR e le incentra principalmente sul titolare e sul responsabile del trattamento. In particolare, l'attenzione che la normativa pone a queste due figure sorprende se confrontata con lo spazio che, nello stesso capitolo, viene dedicato ai diritti dell'interessato, o *data subject*, ossia alla persona fisica a cui si riferiscono i dati personali. Il GDPR, dunque, sembra concentrarsi maggiormente sui diritti e gli obblighi del titolare, o *data controller*, e del responsabile, o *data processor*, andando così a ribaltare la prospettiva della Direttiva 95/46 CE. Se quest'ultima si occupava essenzialmente dell'interessato, regolandone nel dettaglio facoltà ed oneri, il Regolamento opera all'inverso: dove la Direttiva considerava i diritti del *data subject*, il GDPR disciplina doveri e responsabilità degli attori del trattamento[63].

---

[61] Il *Safe Harbor* era l'accordo concluso nel 2000 fra l'Unione Europea e gli Stati Uniti, in virtù del quale i dati personali potevano essere legalmente trasferiti tra i due Paesi per scopi commerciali. Per un'analisi dettagliata del sistema *Safe Harbor,* v. S. Sica, V. D'Antonio, *I Safe Harbor Privacy Principles: genesi, contenuti, criticità,* in *Diritto dell'informazione e dell'informatica*, cit., pp. 80 e ss.

[62] Cfr. A. Schinelli, *Profili critici del trasferimento di dati personali UE-USA tra conflitti regolatori e reazioni politiche*, in S. Bonavita (a cura di), *Società delle tecnologie esponenziali e* General Data Protection Regulation*: la circolazione internazionale dei dati personali*, Milano, Ledizioni, 2018, pp. 2 e ss.

[63] Sul differente approccio adottato dal GDPR rispetto alla Direttiva, v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, vol. I, Torino, Giappichelli, 2016, pp. 153 e ss.

3. Gli attori del trattamento dei dati

L'espressione "trattamento dei dati personali" fa riferimento a <<qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personal*i*>>[64]; in tale operazione rientrano, ad esempio, la raccolta e la conservazione dei dati, così come il loro impiego e la loro diffusione. Come chiarito dalla succitata definizione, dunque, non occorre che il trattamento avvenga con mezzi informatici, né tanto meno che siano poste in essere una pluralità di operazioni: è sufficiente una sola condotta ad integrare la fattispecie, purché questa abbia ad oggetto i dati personali.

Invero, la crescente digitalizzazione della società ha ampliato il novero dei dati personali che possono costituire oggetto di trattamento, sino a ricomprendervi le immagini realizzate dalle telecamere di videosorveglianza, o ancora, i dati ricavati dalle impronte digitali, tali per cui oggi è possibile procedere all'identificazione di una persona. Rendendo possibile la raccolta di un numero sempre maggiore di dati, la rivoluzione informatica ha quindi finito per incidere sulla nozione di dato personale, estendendola a qualunque contenuto informativo, purché riconducibile a una persona fisica identificata, o identificabile[65]. Tuttavia, se questo è vero, è altresì vero che dall'applicazione della disciplina sul trattamento continuano ad essere esclusi i dati "non personali"[66].

Avendo chiarito l'oggetto del trattamento, occorre precisare come, in via generale, esso si connoti per la tensione tra il *data subject* ed altri due soggetti, il *data controller* e il *data processor*, i quali si servono delle informazioni dell'interessato per le proprie finalità. Pur vantando una posizione di diritto sui propri dati, dunque, il *data subject* vede questa comprimersi ogniqualvolta si

---

[64] Ai sensi dell'art. 4, par. 2, del GDPR.

[65] Sulla nozione di dato personale, v. M. Soffientini, *Privacy. Protezione e trattamento dei dati*, Assago, IPSOA, 2018, pp. 4 e ss.

[66] La Commissione Europea definisce i dati non personali come dati « [. . .] *created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real*», v. Commissione Europea, *Communication on Building a European Data Economy*, COM(2017) 9 final, 10 gennaio 2017, p. 9, disponibile *online* su https://digital-strategy.ec.europa.eu/en/library/communication-building-european-data-economy. Tuttavia, la nozione giuridica di dato non personale resta controversa; sul punto, cfr. anche A. Galiano et al., *I dati non personali: la natura e il valore*, in *Rivista Italiana di Informatica e Diritto*, 2020, n. 1, pp. 61 e ss.

relaziona con il *controller* e il *processor*[67]. Ciò nonostante, il rapporto appena descritto è fisiologico del trattamento dei dati; tanto che sia la Direttiva 95/46 CE, che il GDPR, seppur in modo differente, hanno dedicato spazio alle tre figure.

3.1. Il titolare del trattamento o *data controller*

Quanto al titolare e al responsabile del trattamento, malgrado il legislatore italiano adotti termini della tradizione giuridica, non sono altro che le figure che la tradizione anglosassone, sposando un linguaggio informatico, aveva già rispettivamente definito: *data controller*, ossia colui che raccoglie i dati al fine di impiegarli per i propri scopi; *data processor*, cioè chi esegue attività di elaborazione dati per finalità prestabilite[68]. Dal confronto fra le definizioni, in special modo quelle di *data controller* e titolare, emerge come la traduzione italiana rischi di indurre in errore sulla natura di tale soggetto; difatti, il *controller* non ha la titolarità dei dati, i quali restano di proprietà esclusiva dell'interessato, bensì del loro trattamento. Ciò che contraddistingue il titolare è la capacità di determinare le finalità e i mezzi del trattamento[69]. Tali fini, come suggerisce ancora una volta la versione anglosassone, verranno stabiliti per il raggiungimento dei propri obiettivi; si pensi, ad esempio, al gestore di un supermercato che, in qualità di *controller,* tratta i dati forniti dai suoi clienti al solo scopo di fidelizzarli, ovvero fornirgli una "carta fedeltà". Da simili affermazioni è quindi possibile ricavare due concetti fondamentali in relazione al titolare del trattamento. Il primo, è che il ruolo del *data controller* può essere ricoperto tanto da una persona fisica, quanto da una persona giuridica. Infatti, laddove ad utilizzare i dati sia un individuo nell'espletamento della propria professione, la titolarità dei dati sarà riconducibile ad una persona fisica; diversamente, qualora a servirsi dei dati sia un ente pubblico o una società, il titolare sarà individuabile nella persona giuridica *in toto,* pubblica o privata che

---

[67] Così, N. Brutti, *Le figure soggettive delineate dal GDPR: la novità del* Data Protection Officer, in E. Tosi (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali fra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, pp. 118 e ss., il quale sottolinea che <<pur vantando in linea di principio una situazione (o più situazioni) di diritto sui propri dati personali, gli interessati la vedono fisiologicamente compressa e affievolita su più versanti>>.

[68] Sulle definizioni di *data controller* e *data processor*, v. Information Commissioner's Office, *Data controllers and data processors: what the difference is and what the governance implications are*, 2014, disponibile *online* su https://ico.org.uk/media/2698/ico-annual-conference-2014-iain-bourne.pdf.

[69] Ai sensi dell'art.4, par. 7, del GDPR il titolare del trattamento è <<la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali>>.

sia. Sebbene la persona giuridica sia la sola a cui imputare il trattamento, in tali ipotesi le azioni che vogliano essere avviate avverso il *controller*, così come le responsabilità, attive e passive, che vogliano essere fatte valere nei suoi confronti, dovranno essere esercitate nei confronti del legale rappresentante *pro tempore*[70]. Tale conclusione è ormai pacifica; in passato, tuttavia, l'individuazione del *data controller* all'interno di un ente, pubblico o privato che fosse, aveva creato non poche difficoltà interpretative. Invero, un primo orientamento minoritario riteneva che, nel caso della persona giuridica, fosse il rappresentante legale ad assumere il ruolo di titolare. Al contrario, la dottrina prevalente sosteneva che il titolare del trattamento fosse la struttura o l'organismo *in toto*, e non la persona fisica a cui era domandata la rappresentanza. Invero, il riferimento che il Codice della privacy faceva alle persone fisiche[71], in conformità alla vigente Direttiva, non era da imputarsi a coloro che amministrano gli enti, bensì ai soggetti che, a titolo personale, trattano i dati per scopi professionali[72]. Lo stesso Garante per la protezione dei dati personali, d'altronde, ha precisato che <<qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il «titolare» è l'entità nel suo complesso>>[73]. Dunque, non rileva che il *data controller* sia una persona fisica o giuridica, purché vi sia: il titolare, infatti, rappresenta una figura residuale necessaria, non potendo sussistere alcun trattamento dei dati senza che ad esso corrisponda un *controller*[74].

Per quanto concerne il secondo aspetto evincibile dalla nozione di *controller*, esso consiste nella natura funzionale del concetto di titolare. D'altronde, come già anticipato, ciò che contraddistingue tale figura è il potere di definire i mezzi e le finalità del trattamento, ovvero come e perché questo avviene.

---

[70]Per un'analisi approfondita sull'identità e il ruolo del titolare del trattamento, v. R. Panetta, *Gdpr, ecco chi sono (e cosa fanno) il* data controller *e il* data processor, marzo 2018, pp. 4 e ss., disponibile *online* su https://www.corrierecomunicazioni.it/privacy/gdpr/gdpr-ecco-chi-sono-e-cosa-fanno-il-data-controller-e-il-data-processor/.

[71] L'art. 4, lett. f, del Codice della privacy fornisce la definizione di titolare del trattamento, facendovi rientrare qualsiasi persona fisica o persona giuridica, comprese le pubbliche amministrazioni, che determini le finalità e le modalità del trattamento.

[72]Per riscontri di tale tesi nella letteratura italiana, v. F. Garri, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato,* in G. Santaniello (a cura di), *La protezione dei dati personali*, Padova, Cedam, 2005, pp. 136 e ss.

[73] Garante per la protezione dei dati personali, *Chiarimenti sulla Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali*, 9 dicembre 1997, pp.1 e 2, disponibile *online* su https://www.privacy.it/archivio/garanterisp199712092.html.

[74]Cfr. R. e R. Imperiali, *Codice della Privacy*, Milano, Il Sole 24 Ore, 2004, pp. 196 e ss.

Con specifico riferimento alla definizione di "mezzi", è opportuno precisare che la stessa non include soltanto gli strumenti tecnici adoperati nel trattamento, quali *hardware* e *software*, ma in generale il "come", ossia il profilo organizzativo nella sua interezza. Pertanto, nel determinare i mezzi, il titolare spazierà dall'indicare su quali dati incentrare il trattamento e per quanto tempo prolungarlo, all' impartire istruzioni ai suoi subalterni, nonché a dettare misure in ambito di sicurezza[75].

Per quel che riguarda le finalità, invece, ovvero la ragione per cui viene realizzato il trattamento, è fondamentale comprendere chi ne abbia tracciato i confini, giacché questa rappresenta l'unica modalità certa di individuazione del *controller.* Ad un simile risultato, infatti, non si giungerebbe mediante l'adozione di un criterio formale, sia perché spesso l'atto di designazione del titolare è assente, sia perché, quand'anche vi fosse, potrebbe non rispecchiare la situazione effettiva. In quest'ultimo caso, affidandosi alla forma, si rischierebbe di individuare il titolare in qualcuno che non ha affatto potere di determinare il fine[76]. Pertanto, a scanso di equivoci, appare preferibile valutare l'influenza effettiva che un soggetto esercita sulle finalità.

Paradigmatico, in tal senso, è il caso SWIFT, con il quale sono stati messi in discussione il ruolo e le responsabilità che la SWIFT, società belga attiva nel trattamento di messaggi finanziari, ha avuto nel trasferimento di dati personali all'Ufficio per il Controllo degli Asset Esterni (OFAC) del Dipartimento del Tesoro degli Stati Uniti (UST). Difatti, era emerso che dati personali, raccolti e processati tramite la rete SWIFT, erano stati più volte forniti all'UST affinché potesse condurre indagini legate al terrorismo. Così facendo, SWIFT, insieme alle istituzioni

---

[75] Per ulteriori precisazioni sulla definizione di mezzi del trattamento, v. C. Bistolfi, L. Bolognini, E. Pelino, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, pp. 125 e ss.

[76]Per una critica sull'applicazione del criterio formale al *data controller*, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"* (WP 169), 16 febbraio 2010, par. 3.1., lett. a, disponibile *online* su https://www.privacy.it/archivio/grupripareri201001.html, il quale afferma che <<Il concetto di responsabile del trattamento è funzionale, finalizzato cioè all'attribuzione di responsabilità laddove intervenga un'influenza effettiva>>. Nel parere 1/10 il termine "*data controller*" è reso in italiano come "responsabile del trattamento" poiché nella Direttiva 95/46/ CE le espressioni *controller* e *processor* furono tradotte, rispettivamente, come "responsabile" e "incaricato" del trattamento. Ciò, ha provocato non pochi problemi di coordinamento con la normativa interna, secondo la quale il "responsabile", ossia il *controller*, non corrispondeva al soggetto responsabile dell'applicazione della disciplina in materia di protezione dei dati, essendo quest'ultimo, invece, il titolare di trattamento. Tuttavia, il GDPR ha permesso di superare tale divergenza linguistica, traducendo i termini *controller* e *processor* come "titolare" e "responsabile" del trattamento.

finanziarie che se ne servivano, aveva violato le disposizioni della Direttiva 95/46 CE, poiché non aveva informato i clienti che i loro dati sarebbero stati trasferiti negli Stati Uniti a tali fini. Posta la responsabilità della SWIFT e degli altri istituti, il Gruppo dei Garanti europei ha dovuto chiarire, perché questa fosse correttamente ripartita, il ruolo ricoperto da ognuno durante le operazioni di trattamento. Infatti, benché la società belga si presentasse come un intermediario, dal punto di vista della protezione dei dati non si limitava ad avere tale ruolo: negli ultimi anni la SWIFT si era evoluta, cessando di agire esclusivamente per conto dei suoi clienti. Tuttavia, pur volendo ipotizzare che la società di norma operasse come intermediario, e quindi come responsabile del trattamento, nel caso di specie SWIFT aveva assunto responsabilità che andavano oltre l'insieme di istruzioni e doveri a carico di un *processor*. D'altronde, in merito al trasferimento di dati all'UST, SWIFT aveva deciso di conformarsi alle citazioni a comparire dell'autorità federale americana; inoltre, aveva avviato con l'UST negoziazioni in modo non trasparente, omettendo deliberatamente di informare le istituzioni finanziarie interessate. Ebbene, suddetti comportamenti hanno finito per influenzare lo scopo e la portata del trasferimento dei dati all'UST. Pertanto, è indubbio che la SWIFT abbia esercitato poteri che esulano dalle normali capacità di un *processor,* in considerazione dell'assenza di autonomia che tale figura ha rispetto alle istruzioni del titolare. In conclusione, sebbene la SWIFT si presentasse come un responsabile del trattamento, ed alcuni elementi confermassero che in passato aveva agito come tale, il margine di manovra di cui questa godeva nelle operazioni con l'UST dimostra come fosse, in realtà, il titolare del trattamento[77].

Una volta accolto il criterio funzionale, occorre analizzare le circostanze, giuridiche e fattuali, dalle quali si desume chi dispone dell'influenza effettiva e, pertanto, riveste il ruolo di *controller*. In via generale, la qualità di titolare del trattamento può essere ricondotta a quattro fonti differenti. *In primis,* la fonte legale, essendo lo stesso ordinamento giuridico, talvolta, a designare il *controller*. Tale possibilità, d'altro canto, è espressamente prevista dal GDPR, il quale ammette che, laddove le finalità siano stabilite dal diritto dell'Unione Europea, o da quello

[77]Sul caso *SWIFT*, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP128), 22 novembre 2006, parr. 1 e 3.1, disponibile *online* su https://ec.europa.eu/justice/article-29/en.pdf.

nazionale, la figura del titolare sia determinata dalle medesime fonti[78]. Queste ultime potranno quindi designare il *controller* tanto in via diretta, quanto indiretta. Nel primo caso, il titolare viene individuato in maniera puntuale da uno specifico atto normativo[79]; nel secondo, invece, la legge si limita ad attribuire oneri che implicano la gestione di dati, facendo sì che il destinatario di tali obblighi assuma la veste di titolare[80].

La seconda fonte è quella negoziale, ossia vi è un espresso richiamo delle parti contraenti all'identità del titolare; si pensi, ad esempio, ad un contratto di affitto d'azienda in cui la società affittuaria subentri all'affittante nella gestione dell'azienda e, quindi, nel trattamento dei dati che l'attività comporta. In questo caso, è la società affittuaria, dotata di personalità giuridica, a figurare, da contratto, quale titolare del trattamento[81].

Inoltre, può ricorrere l'attribuzione implicita della competenza. Ciò, si verifica quando la qualità di titolare non è prevista per legge né direttamente, né indirettamente, ma deriva da prassi giuridica consolidata. Esemplificativa, in tal senso, è la figura del datore di lavoro, il quale si trova a gestire i dati dei suoi dipendenti; oppure, quella dell'editore, il quale non può astenersi dall'acquisire e disporre dei dati dei propri abbonati. È evidente come, in queste ipotesi, siano i ruoli ricoperti ad indirizzare la scelta del *controller,* giacché la determinazione del trattamento risulta collegata alla funzione assunta nell'organizzazione[82].

---

[78] La designazione del titolare in base alla legge è disciplinata dall'art. 4, par. 7, del GDPR.

[79]A titolo esemplificativo, v. il decreto direttoriale MIUR 24 aprile 2017, n. 941, *Avviso per la selezione delle risorse professionali idonee allo svolgimento delle attività connesse alla realizzazione, al management e alla rendicontazione di progetti di ricerca ERA-Net, CSA, Bandi JTI, Art. 185 e 187 TFUE*, disponibile *online* su http://attiministeriali.miur.it/anno-2017/aprile/dd-24042017.aspx, il quale, all'art. 6, comma 3, precisa che <<titolare del trattamento dei dati personali, ai sensi del d.lgs. n. 196/2003, è la Direzione Generale per il Coordinamento, la Promozione e la Valorizzazione della Ricerca del Ministero>>.

[80]Cfr. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento",* cit., par. 3.1, il quale riporta l'esempio un ente che si occupa di sicurezza sociale e che, a tal scopo, non può non raccogliere dati personali; in tal caso, è la legge ad attribuirgli, indirettamente, il ruolo di titolare del trattamento.

[81]Nella giurisprudenza italiana, v. Cass. 8 aprile 2014, n. 8184, in *Rep. Foro It.,* 2014, voce *Persona fisica e diritti della personalità*, n.124.

[82]A tal proposito, si fa l'ulteriore esempio della trasmissione di un messaggio contenente dati personali attraverso un servizio di telecomunicazione, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento",* cit., par. 3.1). In questo caso, il fornitore di servizi, in virtù della funzione svolta, risulta essere titolare del trattamento solo per i dati relativi al traffico e alla fatturazione, e non per i dati contenuti nel messaggio; infatti, rispetto a questa categoria di dati, il titolare del trattamento è da individuarsi nel soggetto che procede all'invio.

Infine, vi è la fonte fattuale, la cui esistenza non solo ha avuto riconoscimento dottrinale, ma è stata più volte ribadita in ambito giurisprudenziale; difatti, la Suprema Corte ha enucleato il principio secondo cui assume la qualità di titolare colui che abbia determinato i fini e le modalità del trattamento, occupandosi dell'organizzazione dello stesso[83]. Pertanto, il fatto stesso che un soggetto stabilisca le finalità del trattamento può far "scattare" la qualifica di *controller*, pur non essendovi alcun rapporto contrattuale o, addirittura, essendo escluso esplicitamente dal contratto. In tal caso, la titolarità del trattamento viene attribuita in base ad una valutazione delle circostanze di fatto.

Alla luce di tali considerazioni, si può ritenere che le prime tre categorie consentano di individuare con maggiore sicurezza chi sia il titolare, oltre ad essere applicabili alla quasi totalità delle situazioni. Tuttavia, la designazione del *controller*, sia essa legale, negoziale, o per attribuzione implicita, deve comunque trovare riscontro nella realtà fattuale: il titolare sarà quello nominato, o che occupi un dato ruolo nella gestione, solo laddove influenzi effettivamente gli scopi del trattamento dei dati. All'opposto, la fonte fattuale è spesso oggetto di letture divergenti, ragion per cui gli interpreti ricorrono alle condizioni contrattuali, le quali, però, non sempre appaiono decisive. In particolare, le clausole perdono la capacità risolutiva quando ad essere coinvolti nel trattamento sono una pluralità di attori; in quel caso, ancora una volta, occorrerà tenere conto dell'influenza effettiva per trarre una conclusione sulla titolarità. Qualora, invece, nessuna delle categorie citate fosse applicabile, la designazione del *controller* sarebbe da considerarsi nulla, poiché un organismo che non determina, né in via giuridica, né di fatto, le modalità del trattamento non può in alcun modo considerarsi il titolare[84].

Sul *data controller* grava*,* dunque, il compito di fissare a quale scopo i dati personali siano raccolti e, in un secondo momento, utilizzati. Ciò, permette, da un lato, agli interessati di compiere scelte consapevoli in merito ai propri dati, in quanto conoscono il perché del trattamento; dall'altro, ai titolari di individuare le modalità di trattamento più coerenti con le finalità delimitate.

Ebbene, nel definire le ragioni del trattamento, il *controller* agisce secondo il principio di limitazione della finalità del trattamento, il quale è previsto dall'art.

---

[83] In tal senso, v. Cass. 11 giugno 2014, n. 13219, in *Responsabilità Civile e Previdenza,* 2014, n. 4, 1357.

[84]Cfr. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento",* cit., par. 3. 1, lett. a.

5, par. 1, lett. b, del GDPR[85]. In via generale, esso rappresenta uno mezzo di controllo della circolazione dell'informazione, in quanto vincola il trattamento, e con esso il dato che ne è l'oggetto, a un determinato scopo.

Quanto alla *ratio* del principio, essa consiste nella volontà di ricondurre l'interferenza nella sfera privata altrui, conseguenza inevitabile del trattamento dei dati, al perseguimento di finalità meritevoli. Invero, tanto più queste siano ritenute apprezzabili dall'ordinamento, tanto più sarà giustificata l'intromissione nella sfera individuale. Letto alla luce dei criteri di prevedibilità e certezza giuridica, il principio di finalità è stato inoltre considerato alla base di ulteriori principi in materia di protezione dei dati, ossia: il principio di minimizzazione, il principio di esattezza o di limitazione della conservazione, nonché il principio di trasparenza. Ebbene, quello in esame appare un principio di portata generale che trova fondamento nella correlazione fra le ragioni della raccolta dei dati ed il loro uso effettivo. In tal senso, le finalità perseguite dal titolare del trattamento devono essere sempre determinate, esplicite e legittime[86].

Nello specifico, l'espressione "finalità determinate" indica che lo scopo per cui si dispone dei dati deve essere chiaramente e specificamente identificato; ovvero, dettagliato a sufficienza da consentire di definire i tipi di trattamento inclusi o meno nelle finalità, nonché di valutare la conformità di queste ultime alla legge. La determinatezza degli scopi, quindi, richiede una valutazione interna da parte del titolare, il quale dovrà poter dimostrare di aver svolto tale disamina. Ciò, in quanto la scelta di fini specifici rappresenta un passo fondamentale affinché il *controller* garantisca il rispetto della disciplina in materia di protezione dei dati[87].

La locuzione "esplicitezza delle finalità", invece, sta a significare che lo scopo del trattamento, oltre ad essere chiaro al titolare, deve essere espresso in una forma intellegibile. In particolare, occorre che la finalità sia effettivamente esplicata ai soggetti interessati, nonché al *data processor* e alle autorità di protezione dei dati. L'obiettivo del requisito, infatti, è assicurare che gli scopi siano ben specificati, non

[85]Ai sensi dell'art. 5, par. 1, lett. b, del GDPR i dati personali sono <<raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità>>.
[86]Per una riflessione sul principio di limitazione della finalità del trattamento, v. A. Incerti, *Il principio di limitazione della finalità*, in F. Bravo (a cura di), *Dati personali. Protezione, libera circolazione e governance*, vol. I, Pisa, Pacini Giuridica, 2023, pp.203 e ss.
[87]La funzione di garanzia assolta dalla determinazione degli scopi è segnalata dal Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Opinion 03/2013 on purpose limitation,* cit., par. 3.1.1., ove si mette in risalto che << *purpose specification lies at the core of the legal framework established for the protection of personal data*>>.

dovendo residuare alcuna incertezza o difficoltà di comprensione sul loro significato[88]. Per quanto riguarda le modalità di espressione, queste sono alquanto varie, andando a ricomprendere tanto un avviso fornito agli interessati, quanto una notifica all'autorità di vigilanza, così come, a livello interno, informative rese a un responsabile della protezione dei dati.[89]

Infine, occorre che i dati personali siano raccolti per fini legittimi. Tale requisito, tuttavia, non è da riferirsi esclusivamente alle basi giuridiche del trattamento di cui al GDPR[90]; al contrario, va inteso in un'accezione ampia, considerando legittimi gli scopi che siano conformi alla legge in generale. In questo senso, vanno dunque incluse tutte le forme di diritto, sia scritto che consuetudinario, sia di primo che di secondo grado, nonché i principi costituzionali, i diritti fondamentali ed altresì la giurisprudenza, quale legge interpretata dai giudici[91].

3.2. Il responsabile del trattamento o *data processor*

Se quanto asserito sin ora è vero, ossia che il *data controller* è tale finché definisca lo scopo del trattamento, diametralmente opposta è la nozione dell'altro attore del trattamento: il *data processor.* Al pari del titolare, anche la traduzione italiana di *processor*, ovvero responsabile del trattamento, rimanda a concetti della tradizione giuridica, quale quello di illecito aquiliano, rendendo così più difficile coglierne il reale significato. Infatti, il responsabile è <<la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare>>[92]. Da tale definizione emerge chiaramente il ruolo antitetico del *processor* rispetto al *controller*; dove il secondo detta il fine, il primo agisce attenendosi alle finalità di trattamento stabilite. Il rapporto fra titolare e

---

[88]Cfr. A. Ricci, *I diritti dell'interessato*, in G. Finocchiaro (diretta da), *La protezione dei dati personali in Italia*. *Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli,2019, pp.394 e ss.

[89]Sulla varietà di modi con cui esternare gli scopi, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Opinion 03/2013 on purpose limitation,* cit., par. 3.1.2.

[90] L'art. 6 del GDPR elenca le basi giuridiche in virtù delle quali il trattamento è considerato lecito: il consenso dell'interessato, l'esecuzione di un contratto o di misure precontrattuali, l'obbligo legale al quale è soggetto il titolare del trattamento, gli interessi vitali della persona interessata o di terzi, il legittimo interesse prevalente del titolare o di terzi cui i dati vengono comunicati ed, infine, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.

[91] Nel concetto di "legge in generale" si tende ad includere ulteriori elementi, quali le consuetudini, i codici di condotta, i codici etici, le disposizioni contrattuali, nonché il contesto fattuale. Così sembra concepirlo anche il Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Opinion 03/2013 on purpose limitation*, cit., par. 3.1.3.

[92] Ai sensi dell'art. 4, par. 8, del GDPR.

responsabile, quindi, si connota per la strumentalità di quest'ultimo rispetto agli interessi del titolare. Qualora, invece, il *processor* non si limiti ad operare per conto del *controller*, bensì partecipi alla determinazione degli scopi, lo stesso assume la qualifica di titolare, o contitolare, del trattamento. Ancora una volta, pur tenendo in considerazione l'atto di designazione, si applica il criterio funzionale, in quanto si valuta se il *processor,* fuoriuscendo dalle mansioni assegnate, abbia esercitato un'influenza effettiva sulle finalità[93]. D'altronde, la circostanza descritta non è affatto infrequente, tanto che il legislatore europeo ne ha fatto espresso riferimento all'interno del GDPR [94].

Oltre a dover agire per conto del titolare, il responsabile è altresì tenuto ad osservare le sue istruzioni e a sottostare alla sua vigilanza. Difatti, il *processor* è legato al *controller* da un rapporto di preposizione*,* vale a dire il rapporto giuridico mediante il quale il preponente (titolare), con nomina formale, attribuisce al responsabile (preposto) la gestione del trattamento dei dati di sua pertinenza[95]. Proprio in virtù di tale subalternità, come anticipato, il *data processor* è obbligato ad attenersi alle istruzioni del *controller;* infatti, qualora se ne discostasse, e l'inadempimento fosse di non poca rilevanza, egli assumerebbe la veste di titolare.

Dando per assunto che il *processor* sia un preposto del *controller,* è impossibile non notare come il GDPR, a differenza dell'abrogato art. 4 del Codice della privacy[96], non si riferisca mai ad esso in questi termini. Ciò, ha fatto sorgere dei dubbi sulla possibilità che il responsabile sia una figura interna all'organizzazione del titolare. Se, infatti, l'uso del termine preposto rendeva il *processor* perfettamente compatibile con l'articolazione del *controller*, tale sicurezza nel GDPR viene a mancare. Per converso, l'aver specificato che il responsabile agisce <<per conto>>[97] del titolare sembra suggerire che vi sia alterità fra i due. In questo senso, del resto, muovono molti degli obblighi che il GDPR

---

[93]Circa l'applicabilità del criterio funzionale al responsabile del trattamento, v. L. Greco*, L'organigramma privacy: I soggetti del trattamento*, in G. Finocchiaro (diretto da), *La protezione dei dati personali in Italia,* cit., pp. 331 e ss.

[94] Ai sensi dell'art. 28, par. 10, del GDPR <<se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione>>.

[95]Circa la sussunzione della relazione intercorrente tra titolare e responsabile sotto il rapporto giuridico di preposizione, v. M. Massimini, *Il responsabile del trattamento*, febbraio 2006, pp. 2 e ss., disponibile *online* su https://www.privacy.it/archivio/massimini01.html.

[96]L'art. 4, lett. g, del Codice della privacy, abrogato dal d.lgs. 10 agosto 2018, n. 101, definiva il responsabile del trattamento come qualsiasi persona fisica o giuridica, ivi compresa la pubblica amministrazione, che fosse preposta al titolare del trattamento.

[97]Ai sensi dell'art. 4, par. 8, del GDPR.

impone al responsabile nei confronti del titolare, in quanto la maggior parte è già implicita in un rapporto di dipendenza. Si pensi, ad esempio, al dovere del responsabile di informare il titolare qualora sia soggetto a disposizioni incompatibili con le istruzioni da questi impartitegli; tale previsione non avrebbe senso di esistere rispetto ad un *processor* interno*,* poiché dovrebbe sottostare alla medesima disciplina del *controller*. Parimenti, appare difficile comprendere come norme che attribuiscono al responsabile, in via autonoma, sanzioni amministrative, così come quelle che ne riconoscono la responsabilità civile, siano conciliabili con una figura interna[98].

D'altra parte, vi è chi ritiene che il GDPR, se avesse voluto vietare la nomina di *processor* interni, lo avrebbe fatto espressamente. D'altronde, il riferimento al "servizio*"* nella definizione del responsabile non fa che avallare tale tesi. Infatti, sposando la stessa nozione di servizio che era già stata elaborata per il titolare[99], cioè una sottostruttura dotata di poteri decisori posta all'interno di un'organizzazione complessa, si ricava quanto segue: il ruolo del titolare può essere ricoperto anche dal servizio, avendo quest'ultimo la capacità di influenzare il fine; il responsabile può essere tanto esterno, quanto interno[100]. Inoltre, il GDPR ha previsto che il responsabile della protezione dei dati possa essere un dipendente del *controller*, o del *processor*[101]; alla luce di ciò, si potrebbe asserire che il legislatore europeo, non essendosi espresso in senso opposto rispetto al *processor,* abbia voluto implicitamente affermare lo stesso principio. In conclusione, non essendo vietata dal GDPR, non sembra potersi escludere la configurabilità di un responsabile interno, sebbene questa rimanga un'opinione minoritaria[102].

---

[98] La letteratura in tema di incompatibilità del *processor* interno con il GDPR è copiosa, per tutti: D. Farace, *Il titolare e il responsabile del trattamento*, in V. Cuffaro et al. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, pp. 759 e ss.

[99] In merito alla figura del titolare, il Garante per la protezione dei dati personali, ha specificato che la direzione generale, o area, la quale eserciti un potere decisionale sulle finalità del trattamento, assume il ruolo di titolare del trattamento e che, in tale categoria, devono essere altresì ricompresi i servizi (v. *Chiarimenti sulla Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali*, cit., p. 2.)

[100]A favore del responsabile quale figura interna all'organizzazione del titolare, v. C. Bistolfi, L. Bolognini, E. Pelino, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali,* cit., pp. 124 e ss.

[101]Ai sensi dell'art. 37, par. 6, del GDPR <<il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi>>.

[102]Su posizioni sostanzialmente analoghe, v. L. Greco, *I ruoli: titolare e responsabile*, in G. Finocchiaro (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, Zanichelli, 2017, pp. 278 e ss.

In virtù del Regolamento, il responsabile del trattamento deve altresì presentare <<le garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato>>[103]. La normativa, quindi, richiede che il *processor* sia dotato di un'attitudine professionale, ossia che possieda competenze specifiche in materia di protezione dei dati. La professionalità rappresenta un aspetto imprescindibile del responsabile; difatti, quand'anche il GDPR non lo avesse previsto, il titolare avrebbe dovuto egualmente procedere a valutarlo. Ciò, in primo luogo, perché il *data controller* risponde alle autorità anche di azioni commesse da altri, ivi compreso il responsabile. Pertanto, è evidente l'interesse del titolare a servirsi di collaboratori competenti, oltre che a disporre clausole *ad hoc* per la ripartizione interna delle responsabilità. In secondo luogo, il *controller* deve assicurare sia che vengano adottate misure tecniche e organizzative tali per cui il trattamento sia conforme al GDPR; sia che, durante il periodo in cui egli dispone dei dati, siano tutelati i diritti dell'interessato. A tal fine, occorre che il titolare valuti attentamente le conoscenze del responsabile, in quanto detti obiettivi sono raggiungibili solo affidando il trattamento a chi abbia competenze specifiche[104].

Nonostante il GDPR abbia definito i requisiti del *data processor*, quest'ultimo, a differenza del *controller*, non è una figura necessaria; al contrario, egli si caratterizza per la facoltatività. Tale aspetto, in realtà, non stupisce se si considera che già la normativa previgente, sia europea, che nazionale, indicava la nomina del responsabile quale facoltativa. In particolare, il Codice della privacy prevedeva che il titolare "potesse" servirsi di un responsabile e che, per particolari esigenze organizzative, "potesse" attribuire tale ruolo a più soggetti[105]. Allo stesso modo, il GDPR menziona il trattamento ad opera del responsabile come un'ipotesi meramente eventuale[106]. Ciò nonostante, sempre più spesso si assiste alla nomina di un *processor* da parte del *controller*, potendo questo non avere il tempo

[103]Il requisito necessario di cui deve disporre il *processor*, ossia la capacità di adottare misure tecniche e organizzative adeguate, è disciplinato ai sensi dell'art. 28, par. 1, del GDPR.
[104] Circa il requisito di professionalità del responsabile del trattamento, v. F. De Stefani, *Le regole della privacy. Guida pratica al nuovo GDPR*, Milano, Hoepli, 2018, pp. 19 e ss.
[105] Ai sensi dell'art. 29, comma 3, del Codice della privacy, abrogato dal d.lgs. 10 agosto 2018, n. 101, <<ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti>>.
[106]Ai sensi dell'art. 28, par. 1, del GDPR.

necessario o, ancora più importante, le capacità organizzative, per gestire il trattamento. In siffatta ipotesi, la nomina del *processor* diviene la prima misura idonea a contrastare i rischi connessi all'attività di trattamento; pertanto, è raro che il titolare, la cui organizzazione presenti un minimo di complessità, non ne designi alcuno[107].

3.3. Il sub-responsabile del trattamento

Se è vero che il titolare ha la tendenza a servirsi di almeno un responsabile del trattamento, è altresì vero che questo, a sua volta, può attribuire parte dei suoi compiti a soggetti esterni: i sub-responsabili.

Per quel che riguarda tale figura, occorre rilevare come, prima dell'entrata in vigore del GDPR, non vi fosse alcun riferimento normativo in proposito, né europeo, né tanto meno nazionale. Tuttavia, un utile contributo alla materia era pervenuto dal Gruppo di lavoro "Articolo 29", il quale aveva precisato che, qualora il trattamento dei dati fosse affidato a degli esterni, gli obblighi e le responsabilità derivanti dalla legge sulla protezione dei dati sarebbero comunque stati da ripartire in modo chiaro, non dovendo <<disperder[si] lungo la catena di esternalizzazione e di subcontraenti>>[108]. Dunque, a parere del Gruppo, era preferibile evitare di ricorre ad una pluralità di sotto-incaricati, salvo che non vi fosse una chiara ripartizione delle responsabilità e ne fosse debitamente informato il titolare. Malgrado non fosse espressamente previsto, già il Gruppo di lavoro riteneva opportuno che il titolare fosse messo al corrente di eventuali sub-responsabili, nonché del trattamento che venisse loro affidato; difatti, questo era l'unico modo che il *controller* aveva di continuare a vigilare sui dati trattati per suo conto.

Allo stesso modo, il contesto nazionale era privo di un atto normativo che disciplinasse il sub-responsabile; ciò nonostante, la possibilità che il responsabile provvedesse alla sua nomina fu contemplata dal Garante nazionale per la protezione dei dati. Quest'ultimo, infatti, nell'ambito di un provvedimento sul trattamento dei dati mediante sistema di monitoraggio a distanza per pazienti con defibrillatori cardiaci impiantabili attivi (Provvedimento Rfid), aveva fornito importanti

[107]Così G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Bologna, Zanichelli, 2012, p. 85.
[108]Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, cit., par. 3. 2.

chiarimenti in materia; tanto che, pur essendo un atto specifico, ed avendo il Garante esteso la sua applicazione solo a trattamenti analoghi, ha rappresentato il testo di riferimento in Italia fino all'adozione del GDPR. Il provvedimento, infatti, non si limitava ad ammettere che il responsabile nominasse dei subappaltatori in qualità di sub-responsabili, ma ne dettava le condizioni. Preliminarmente, il *processor* doveva informare il *controller* che avrebbe coinvolto terzi nell'espletamento di alcune attività per suo conto, così da ottenerne il consenso. A quel punto, i sub-responsabili, mediante accordo scritto, si impegnavano a rispettare gli stessi obblighi che il responsabile aveva nei confronti del titolare. Quindi, il *processor* rendeva copia al *controller* di tali contratti e si onerava di tenerne un elenco aggiornato[109].

Visto il vuoto normativo che caratterizzava la materia, è evidente come una delle novità più rilevanti del GDPR sia quella di aver regolato la figura del sub-responsabile. In tale regolazione, tuttavia, ricorrono molti degli elementi presenti nelle linee guida del Garante, fra cui la circostanza che il *processor* incarichi i sub-responsabili solo previa autorizzazione scritta del titolare. Quanto al contenuto, secondo il GDPR, essa può individuare espressamente il sub-responsabile, e quindi essere specifica, oppure non fornire alcun nominativo, ed essere cioè generale. In tal caso, il responsabile è tenuto a comunicare al titolare ogni aggiunta o sostituzione del sub-responsabile, poiché il *controller* vanta un diritto di opposizione in merito[110]. Benché lo riconosca, il Regolamento non fissa un limite temporale all'esercizio di questo diritto, ragion per cui si ritiene validamente azionato entro un termine congruo, ovvero purché non arrechi danno al regolare svolgimento dell'attività dei soggetti coinvolti[111].

Inoltre, al pari del Provvedimento Rfid, il GDPR impone ai responsabili e ai sub-responsabili di concludere un contratto, o altro atto giuridico, recante i medesimi obblighi di *data protection* previsti dal contratto fra titolare e

---

[109] Cfr. Garante per la protezione dei dati personali, *Trattamento dei dati personali attraverso un sistema "Rfid" di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Verifica preliminare richiesta da Azienda Ospedaliera e Sas - 29 novembre 2012 [2276103]*, disponibile *online* su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2276103.

[110] Il requisito dell'autorizzazione scritta del titolare del trattamento ed il diritto di opposizione di quest'ultimo sono previsti ai sensi dell'art. 28, par. 2, del GDPR.

[111] Sul termine per l'esercizio del potere di opposizione del titolare, v. A. D'Ottavio, *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, Giuffrè, 2019, pp. 172 e ss, il quale afferma che, in *silentio legis*, le parti possono altresì concordare il termine in sede di autorizzazione generale.

responsabile. Nello specifico, si richiede che l'atto disponga <<garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento>>[112].

Pur avendo regolato la figura del sub-responsabile, il GDPR non gli attribuisce espressamente la facoltà di nominare, a sua volta, un soggetto esterno, in modo da costituire una vera e propria "catena di sub-responsabili". Eppure, non lo vieta; di conseguenza, è presumibile che un simile scenario si verifichi nella realtà aziendale, essendo quest'ultima caratterizzata da una struttura multilivello.

3.4. L'incaricato del trattamento

Parimenti, il Regolamento non contempla la figura dell'incaricato del trattamento, la quale era invece espressamente prevista dal Codice della privacy[113]. Malgrado ciò, è indubbio che suddetta figura sia compatibile con il GDPR, dal momento che lo stesso obbliga al rispetto delle istruzioni del titolare sia il responsabile, che <<chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento>>[114]. Ebbene, nell'ammettere che altri soggetti possano affiancare il titolare e il responsabile del trattamento, il GDPR non fa altro che disciplinare la figura dell'incaricato del trattamento. Quest'ultimo, infatti, è la persona fisica chiamata ad eseguire materialmente le operazioni che derivano dal trattamento dei dati, nel rispetto delle istruzioni del *data controller* e del *data processor*. Pertanto, non si riscontra alcuna preclusione alla "nomina" dell'incaricato del trattamento; al contrario, questo viene visto con favore dal GDPR, poiché rende più agevole per il titolare rispettare il principio di *accountability*[115].

D'altronde, il *favor* che il Regolamento nutre nei confronti dell'incaricato emerge da un ulteriore aspetto: l'assenza di norme sulle modalità di delega di quest'ultimo. Il GDPR, infatti, non prevede che l'incaricato debba essere designato

[112] Ai sensi dell'art. 28, par. 4, del GDPR.
[113] Ai sensi dell'art. 30, comma 1, del Codice della privacy, abrogato dal d.lgs. 10 agosto 2018, n. 101, <<le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite>>.
[114] Ai sensi dell'art. 29 del GDPR.
[115] Così A. D'Ottavio, *op. ult. cit*., pp. 180 e ss. Nella stessa direzione si è espresso il Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali*, febbraio 2018, pp. 23 e ss., disponibile *online* su https://www.unich.it/sites/default/files/guida_all_applicazione_del_regolamento_ue_2016_679.pdf , il quale sostiene che le disposizioni del Codice della privacy in materia di incaricati del trattamento siano perfettamente compatibili con la struttura e la *ratio* del GDPR.

per iscritto, purché risulti in modo chiaro l'ambito di trattamento dei dati in cui sia consentito il suo operato. Allo stesso modo, l'art. 2 *quaterdecies*, comma 2, del Codice della privacy stabilisce che <<il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta>>. La scelta di come incaricare un soggetto terzo, quindi, viene totalmente rimessa al *controller* o al *processor*, i quali potrebbero tanto adottare un separato atto di nomina o un atto bilaterale, quanto optare per un a*ddendum* al contratto di lavoro già esistente o, per sino, farvi un mero rinvio. In ogni caso, essi sono tenuti a specificare l'oggetto della delega[116].

4. Il principio di *accountability.* Una rivoluzione nella regolazione della *data protection*

Per quanto concerne il suddetto principio, esso rappresenta una delle innovazioni più rilevanti che il GDPR ha apportato alla materia della protezione dei dati, in quanto non era stabilito dalla previgente disciplina europea. La Direttiva 95/46 CE, infatti, si era limitata a prevedere che il *controller* garantisse il rispetto degli oneri di cui all'art. 6, par. 1[117], arrestandosi ad una forma "embrionale" di responsabilizzazione dello stesso. Inoltre, tale disposizione non aveva mai trovato attuazione nella normativa italiana, la quale né nella legge 31 dicembre 1996, n. 675, né nel successivo d.lgs. 30 giugno 2003, n. 196 aveva fatto riferimento alla responsabilizzazione del titolare.

---

[116] Sulla figura dell'incaricato del trattamento e sulla sua designazione, v. F. Lorè*, Il responsabile del trattamento. Privacy e "cura" dei dati in sanità*, in *Giornale Italiano di Nefrologia,* 2019, n. 2, pp. 5 e ss.

[117]Ai sensi dell'art. 6, par. 1, della Direttiva 95/46 CE <<gli Stati membri dispongono che i dati personali devono essere:
a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non in compatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successiva mente trattati, cancellati o rettificati;
e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici>>.

Nonostante il principio di *accountability* fosse quasi totalmente sconosciuto alla legislazione europea, e del tutto a quella nazionale, era stato oggetto di studio del Gruppo di lavoro "Articolo 29". Quest'ultimo, nello specifico, aveva rilevato quanto fosse complesso trasporre il termine *accountability* nelle altre lingue, giacché poteva assumere una pluralità di significati: responsabilità, affidabilità, assicurazione, obbligo di rendicontazione. Tuttavia, il Gruppo aveva chiarito che, comunque lo si traducesse, il principio in esame mirava a valorizzare due aspetti: <<[la] dimostrazione di come viene esercitata la responsabilità e [la] sua verificabilità>>[118]. Invero, il principio di *accountability* poteva dirsi attuato allorché il *data controller* avesse adottato misure idonee a conformarsi agli altri principi in materia di *data protection* e fosse stato, altresì, in grado di dimostrarlo[119].

A livello internazionale, invece, il concetto di *accountability* compare per la prima volta nelle Linee Guida OCSE del 1980, ove si affermava che <<*a data controller should be accountable for complying with measures which give effect to the principles stated above*>>[120]. Diversamente, non vi era menzione della responsabilizzazione del titolare nella prima versione della Convenzione 108; solo con il Protocollo[121] emendativo della citata convenzione, infatti, il principio di *accountability* ha fatto il suo ingresso nel diritto internazionale. In particolare, la Convenzione onerava il titolare e il responsabile di adottare le misure necessarie ad attuare gli obblighi ivi prescritti; nonché, di provare che il trattamento dei dati avvenisse in maniera conforme alla Convenzione. Ancora, era previsto che il *controller*, così come il *processor,* prevedesse l'impatto che il trattamento avrebbe avuto sui diritti e le libertà dei *data subject*, in modo da elaborare un trattamento che azzerasse, o comunque riducesse al minimo, i rischi per i diritti degli interessati. Inoltre, la Convenzione statuiva che, ogniqualvolta il titolare ed il responsabile

---

[118] Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 3/2010 sul principio di responsabilità* (WP 173), 13 luglio 2010, par. 2.21, disponibile *online* su https://www.privacy.it/archivio/grupripareri201003.html#:~:text=Il%20Gruppo%20di%20lavoro%20art.%2029%20rileva%20che%20alcuni%20responsabili,difficile%20situazione%20economica%20dell'UE.

[119] Gruppo Art. 29, *op. ult. cit*., par. 3.2.28.

[120] OECD, *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* OECD/LEGAL/0188, 23 settembre 1980, p. 8, disponibile *online* su https://legalinstruments.oecd.org/public/doc/114/114.en.pdf.

[121] Cfr. Comitato dei Ministri, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108),* 17-18 Maggio 2018, disponibile *online* su https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52018PC0449.

avessero voluto adottare misure tecniche ed organizzative, avrebbero dovuto valutarne le implicazioni con il diritto alla protezione dei dati[122].

Alla luce di ciò, emerge una differenza fondamentale fra il principio di *accountability* contemplato dalla Convenzione e quello previsto dal GDPR: la prima estende il principio anche al *data processor,* mentre il secondo lo riferisce esclusivamente al *controller*[123].

Volendo fornire una definizione del termine *accountability,* questo può essere inteso allo stesso tempo come responsabilizzazione e prova della responsabilizzazione; talvolta, è altresì tradotto come principio di rendicontazione o di responsabilità. Al di là dell'espressione scelta, però, è pacifico che il principio di *accountability* sia presente in più di una disposizione del Regolamento. Sebbene la norma di riferimento sia considerata l'art. 24 del GDPR, il quale onera il *data controller* di adottare misure idonee a conformarsi al Regolamento e, se richiesto, di dimostrarlo, il principio di *accountability* permea l'intero *corpus* del GDPR. Si pensi, a titolo esemplificativo, all'art. 5, par. 2, del Regolamento, il quale dispone che <<il titolare del trattamento è competente per il rispetto del paragrafo 1 [dei principi applicabili al trattamento dei dati personali] e in grado di comprovarlo (responsabilizzazione*)*>>. Tale norma va chiaramente a riassumere il duplice profilo, prescrittivo e probatorio, che connota il principio di *accountability.*

I medesimi aspetti vengono riproposti ancora dal legislatore in relazione alle misure di sicurezza[124], nonché ogniqualvolta siano richieste al titolare delle valutazioni: ad esempio, quelle sul legittimo interesse come base giuridica del trattamento[125], o quelle da effettuare in seguito ad un *data breach*[126].

---

[122]Il principio di *accountability* e gli oneri che da esso derivano in capo al titolare e al responsabile del trattamento sono regolati ai sensi dell'art. 8, parr. 1, 2 e 3, della Convenzione 108.

[123]Per un'attenta analisi sul principio di *accountability* e sulla sua introduzione all'interno del panorama normativo europeo, v. F. Albanese, I. Cardinali*, Il principio di responsabilizzazione (*accountability*),* in F. Bravo (a cura di), *Dati personali. Protezione, libera circolazione e* governance, cit., pp. 507 e ss.

[124] Ai sensi dell'art. 32, par. 1, del GDPR, il titolare e il responsabile del trattamento sono tenuti ad adottare misure tecniche e organizzative tali da assicurare un livello di sicurezza adeguato al rischio <<tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche>>.

[125] L'art. 6, par. 1, lett. f, del GDPR, prevede che il titolare possa prescindere dall'acquisizione del consenso qualora il trattamento sia necessario per il raggiungimento del suo legittimo interesse, purché non prevalgano i diritti o le libertà fondamentali del *data subject,* i quali richiedono la protezione dei dati personali.

[126]Per quanto concerne il *data breach,* l'art. 33, par. 1, del GDPR impone al titolare l'obbligo di notificare la violazione dei dati personali all'autorità di controllo competente, salvo che la stessa non costituisca in alcun modo un rischio per i diritti e le libertà delle persone fisiche.

Oltre ad interessare le singole norme, il principio di responsabilizzazione permea anche i considerando del GDPR. Difatti, il considerando n. 74 fa espresso richiamo ad entrambi gli obblighi del *controller*, ossia impiegare misure efficaci nel trattamento e poterne dimostrare la conformità al Regolamento. Parimenti, i considerando n. 77 e 78 sottolineano il profilo probatorio, prevedendo che, a tal scopo, il titolare possa ricorrere a: codici di condotta e certificazioni; politiche interne che soddisfino i principi della protezione dei dati sin dalla progettazione.

Dalla disamina delle norme, è evidente che l'adozione del principio in esame ha rivoluzionato l'impianto generale della normativa sulla *data protection*; infatti, pur garantendo la continuità con alcune delle disposizioni previgenti, il GDPR ha segnato il passaggio <<da un approccio normativo fondato su regole assai dettagliate, ad uno basato su principi e volto a responsabilizzare il titolare del trattamento>>[127].

Benché, ad esempio, il Regolamento riproponga le disposizioni sull'informativa e sul consenso, queste sono ora inserite in un contesto normativo profondamente diverso, perché basato sul principio di *accountability*. Ciò, emerge dall'art. 12 del GDPR, ove il legislatore prevede che gli interessati ricevano tutte le informazioni relative al trattamento; tuttavia, la scelta di come debbano essere trasmesse è rimessa ad un unico soggetto: il titolare del trattamento. Ancora, rispetto alla base giuridica del trattamento, il Regolamento dispone che sia il titolare ad individuare quale ricorra nel caso di specie e, conseguentemente, comunicarlo all'interessato[128]. In particolare, quanto al consenso del data *subject,* il *controller* deve poter dimostrare di averlo effettivamente acquisito, avendo totale libertà nella scelta dei mezzi di prova[129]. Diversamente, il previgente Codice della privacy riconosceva il consenso quale base giuridica purché liberamente prestato e specificatamente rivolto ad un trattamento; in aggiunta, questo doveva essere <<documentato per iscritto>> e, in caso di dati sensibili, <<manifestato per iscritto>>[130].

---

[127]R. Caterina, *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in *Giurisprudenza Italiana*, 2019, n. 12, p. 2777.

[128]L'onere di rilevare la base giuridica del trattamento è posto in capo al titolare dall'art. 13, lett. c, del GDPR.

[129] Ai sensi dell'art. 7, par. 1, del GDPR <<qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali>>.

[130]Il consenso quale requisito di legittimità del trattamento era disciplinato dall'art. 23, commi 2 e 3, del Codice della privacy, abrogato dal d.lgs. 10 agosto 2018, n. 101.

L'ambito in cui si notano maggiormente gli effetti del principio di *accountability* è quello della sicurezza dei dati. Difatti, in epoca antecedente al GDPR, il legislatore tendeva ad individuare espressamente quali misure di sicurezza dovessero essere adottate; in tal senso, il disciplinare tecnico, di cui all'allegato B del Codice della privacy, elencava le misure minime per non incorrere nella responsabilità penale. La normativa vigente, invece, riporta una prescrizione di carattere generale, indicando soltanto i criteri alla luce dei quali selezionare le misure di sicurezza: lo stato dell'arte, i costi di attuazione, la natura, l'oggetto, il contesto, le finalità del trattamento, nonché il rischio per i diritti e le libertà delle persone fisiche[131]. Il titolare, quindi, non può esimersi dal considerare tali elementi nell'adottare le misure di sicurezza adeguate. Tuttavia, gli oneri del *controller* non si riducono ad un'analisi preventiva e a una valutazione successiva, essendo questi tenuto a monitorare, nel tempo, l'efficacia e la proporzionalità al rischio delle misure scelte. Inoltre, durante l'intero trattamento, il titolare è chiamato ad agire nel rispetto della disciplina sulla *data protection* e a poterne dare prova.

Malgrado sembrino coincidere con quelle della Direttiva, le previsioni del GDPR sono in realtà connotate da un significato differente, frutto del diverso contesto normativo in cui si collocano: interamente orientato al principio di *accountability*[132].

In virtù di tale principio, il *data controller* è tenuto a configurare un sistema di controllo della protezione dei dati che, da un lato, rispecchi standard di buona amministrazione universalmente riconosciuti; dall'altro, sia sottoponibile a una verifica esterna. Infatti, perché il trattamento sia conforme alla disciplina sulla *data protection*, il titolare non può limitarsi ad attuare le norme di legge, ma occorre che predisponga <<una vera e propria *governance* interna>>[133].

In quest'ottica, si richiede al *controller* di tutelare, contemporaneamente, i dati personali e i diritti dei soggetti coinvolti nel trattamento, come emerge dalle disposizioni sulla progettazione e protezione per impostazione predefinita.

---

[131]I canoni da seguire nella scelta delle misure di sicurezza sono previsti dall'art. 32, par. 1, del GDPR.

[132]In tal senso G. Finocchiaro, *GDPR tra novità e discontinuità - Il principio di* accountability, in *Giurisprudenza Italiana*, cit., pp. 2779 e ss., la quale ritiene che il legislatore europeo, alla luce del principio di responsabilizzazione, abbia modificato <<significativamente l'approccio sostanziale>>.

[133]A. Spina, *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al Regolamento (UE) 2016/67,* in *Rivista della Regolazione dei mercati*, 2016, n. 1, p. 148.

All'interno del GDPR, viene quindi ad essere regolato il principio della privacy *by default*, volto a tutelare la vita privata per impostazione predefinita, e della privacy *by design*, il quale mira a garantire i dati sin dalla loro progettazione[134]. Quest'ultimo, in particolare, dispone che la tutela dei dati sia assicurata a decorrere dalle fasi di sviluppo e pianificazione del trattamento; pertanto, il *controller,* prima ancora che l'attività abbia inizio, è chiamato a considerare l'impatto che il trattamento avrebbe sull'interessato. Una valutazione *ex ante*, d'altronde, permette al titolare di trattare i dati riducendo al minimo le conseguenze per il *data subject*; inoltre, gli consente di comprendere, già in fase di progettazione, quali norme del GDPR seguire nelle sue attività future.

Affinché il principio di privacy *by design* trovi attuazione, il titolare è chiamato ad adottare misure tecniche ed organizzative idonee sia a rispettare la normativa vigente, che ad offrire tutela all'interessato. Pertanto, in fase di progettazione, il *data controller* che intenda avviare un trattamento provvede: in via preliminare, ad individuare i dati coinvolti nella realizzazione del nuovo prodotto o servizio; di seguito, a circoscrivere la raccolta dei dati a quelli necessari per il raggiungimento dell'obbiettivo (cd. minimizzazione dei dati). Ancora, è richiesto al titolare di stabilire il periodo di conservazione dei dati in relazione alla durata del trattamento e a quanto stabilito, sul punto, dalla normativa vigente. Oltre al termine, il *controller* è tenuto ad indicare, già in sede di pianificazione, chi sono gli addetti al trattamento ed il ruolo che ricoprono, ovvero di responsabili o incaricati del trattamento[135]. In definitiva, <<i modelli di privacy *by design* si fondano su un approccio proattivo alla tutela dei dati personali >>[136], preferendo un meccanismo di privacy basato su una tutela *ex ante* delle situazioni soggettive, piuttosto che uno incentrato sulla tutela, *ex post,* del danno.

Il principio di *accountability* si configura allora come una forma di responsabilizzazione, o responsabilità *ex ante*, dei soggetti attivi del trattamento, introdotta dal legislatore per conferire centralità tanto al titolare, quanto al

---

[134] I principi di privacy *by design* e privacy *by default* sono espressamente regolati dall'art. 25 del GDPR, il quale è rubricato <<protezione dei dati fin dalla progettazione e protezione per impostazione predefinita>>.

[135]Sugli adempimenti connessi al principio di privacy *by design*, v. E. Faccioli, M. Cassaro, *Il "GDPR"e la normativa di armonizzazione nazionale alla luce dei principi:* accountability *e privacy* by design, in *Diritto industriale*, 2018, n. 6, pp. 563 e ss.

[136] R. Carleo, *Il principio di* accountability *nel GDPR: dalla regola alla auto-regolazione**, in R. Carleo, A.M. Gambino, M. Orlandi (diretto da), *Nuovo Diritto Civile*, 2021, n. 1, p. 373.

responsabile. In questa prospettiva, il GDPR ha ampliato gli oneri gravanti sulle due figure in virtù della disciplina previgente[137].

Per quanto concerne il titolare del trattamento, è indubbio che la Direttiva 95/46 CE gli indirizzasse una pluralità di obblighi: alcuni di risultato, quale quello di raccogliere dati per scopi legittimi e non elaborarli in modo incompatibile con gli stessi[138]; altri di mezzi, come quello di adottare <<tutte le misure ragionevoli>>[139] affinché i dati inesatti fossero rettificati o cancellati. Allo stesso modo, l'art. 17, par. 1, della Direttiva imponeva al *controller* di <<attuare misure tecniche e organizzative appropriate>> al fine di garantire la riservatezza e la sicurezza del trattamento. Quest'ultima, d'altronde, costituiva il fulcro degli oneri del titolare che, pur essendo molteplici, ruotavano attorno ad unico ambito: le misure di sicurezza.

La Direttiva, inoltre, attribuiva al *controller* il dovere generale di garantire che il trattamento fosse conforme alla disciplina in vigore. Alla base di tale obbligo vi era l'idea che il *processor* fosse un mero esecutore, il cui unico compito era osservare le istruzioni del titolare. In altre parole, la Direttiva imponeva al *controller* un obbligo di diligenza non delegabile nei confronti degli interessati, cioè che non poteva essere trasferito a un contraente indipendente. Pertanto, il solo fatto che l'azione illecita fosse compiuta dal *processor*, piuttosto che dal *controller*, non diminuiva la responsabilità di quest'ultimo. All'opposto, il titolare era responsabile per qualunque violazione della Direttiva, a prescindere che fosse stata perpetrata da lui in prima persona, o dal responsabile.

In tale ottica, la Direttiva 95/46 CE non contemplava nessuna disposizione che regolasse la responsabilità del *processor*. A quest'ultimo, del resto, non veniva attribuito alcun obbligo diretto, salvo quello di cui all'art. 16, ovvero elaborare i dati seguendo pedissequamente le istruzioni del titolare. Qualora il titolare avesse voluto imporre al responsabile ulteriori oneri, sarebbe quindi dovuto ricorrere alla via negoziale. Infatti, l'art. 17, par. 3, prevedeva che il *controller* incaricasse il responsabile mediante un contratto, o altro atto giuridico vincolante, di cui la Direttiva si limitava a dettare il contenuto minimo: l'obbligo per il *processor* di attenersi sempre alle istruzioni del *controller*, nonché di adottare misure tecniche e

[137] Cfr. L. Greco, *I ruoli: titolare e responsabile*, cit., pp. 279 e ss.
[138] Ai sensi dell'art. 6, par. 1, lett. b, della Direttiva 95/46 CE.
[139] Ai sensi dell'art. 6, par. 1, lett. d, della Direttiva 95/46 CE.

organizzative atte a garantire la sicurezza del trattamento[140].

4.1. La responsabilizzazione degli attori del trattamento fra Direttiva 95/46 CE e GDPR

Alla luce di tali considerazioni, appare lampante <<la differenza non solo di disciplina, ma anche di approccio del Regolamento rispetto alla normativa previgente>>[141].

Laddove la Direttiva incentrava gli oneri del *controller* attorno alle misure di sicurezza, il Regolamento attribuisce a quest'ultimo obblighi relativi ad una pluralità di ambiti; si pensi, ad esempio, ai citati principi di privacy *by design* e privacy *by default*, la cui implementazione è rimessa proprio al titolare. Questi, inoltre, deve occuparsi della consultazione preventiva e della tenuta del registro, nonché degli adempimenti connessi alla *data breach notification.* Nello svolgimento di tali compiti, il *controller* assume una posizione di centralità, che diviene esclusiva ogniqualvolta il responsabile non possa agire per suo conto.

Al di là di ampliare gli obblighi del titolare, Il GDPR modifica quanto già previsto rispetto alla salvaguardia del trattamento. La Direttiva, infatti, imponeva al titolare di attuare, nel corso del trattamento, misure di sicurezza che scongiurassero eventuali violazioni dei dati personali. Il Regolamento, invece, adottando un nuovo approccio al rischio, prevede che il titolare configuri misure di sicurezza prima ancora di poter disporre dei dati. Solo così, del resto, l'azione del *controller* può dirsi conforme alla progettazione e protezione per impostazione predefinita. Nella medesima ottica di tutela anticipata, il GDPR richiede al titolare di dotarsi di una valutazione d'impatto del trattamento[142].

---

[140]Sulla ripartizione di obblighi fra titolare e responsabile del trattamento secondo la Direttiva 95/46 CE, v. B. Van Alsenoy, *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. VII, 2016, n. 3, pp. 273 e ss.

[141] L. Greco, *I ruoli: titolare e responsabile*, cit., p 281.

[142] La Valutazione d'Impatto sulla Protezione dei Dati (DPIA) è un requisito introdotto dall'art. 35 del GDPR, in attuazione del principio di privacy *by design*. Secondo il Regolamento, l'adozione della DPIA è necessaria quando un determinato trattamento, a causa delle tecnologie impiegate, nonché per la natura, la portata, il contesto e gli scopi che lo caratterizzano rappresenta un rischio per i diritti e le libertà delle persone fisiche. Pertanto, il titolare del trattamento, prima che questo abbia inizio, è tenuto a valutare l'incidenza che le operazioni previste potrebbero avere sulla protezione dei dati personali. A tal proposito, v. M. Boban, *GDPR and Data Protection Impact Assessment (DPIA),* in M. Milkovic, K. Hammes, O. Bakhtina (a cura di), *Economic and Social Development (Book of Proceedings),* Varaždin, Varazdin Development and Entrepreneurship Agency, 2020, pp. 215 e ss.

Accanto a tali novità, il Regolamento stabilisce che il titolare non solo agisca nel rispetto nella normativa, ma sia anche in grado di darne prova. Una previsione di questo tipo appare pienamente in linea con l'impostazione del GDPR, tutto orientato al principio di *accountability.* D'altro canto, questa è la *ratio* che sottostà a molti dei neo-introdotti oneri del *controller*, non in ultimo, la tenuta del registro delle attività di trattamento[143].

Relativamente alla figura del titolare, il Regolamento ha realizzato un intervento notevole; tuttavia, ancor più dirompente è stato quanto stabilito in merito al responsabile. Come anticipato, infatti, la Direttiva non destinava al *processor* alcuna previsione, fuorché quella di conformarsi alle istruzioni del titolare e di essere nominato, da quest'ultimo, mediante atto giuridico vincolante. Il GDPR, discostandosi da un simile approccio, ha invece indirizzato al responsabile diversi obblighi, stabilendone altresì la personale responsabilità in caso di inottemperanza. Alla luce di ciò, si assiste alla maturazione della figura del responsabile, il quale non è più mero esecutore per conto del titolare, bensì un soggetto pienamente responsabile delle sue azioni.

In conclusione, occorre rilevare come le citate innovazioni, ossia aver inasprito gli obblighi del titolare ed avergliene attribuiti di nuovi, nonché aver riservato al responsabile previsioni *ad hoc,* costituiscano il mezzo adoperato dal GDPR per raggiungere un obbiettivo: la responsabilizzazione dei soggetti attivi del trattamento[144].

[143]Il registro delle attività di trattamento, così come disciplinato dall'art. 30 del GDPR, è uno strumento atto a fornire il quadro dei trattamenti in essere presso il titolare. Pertanto, il registro rappresenta un mezzo indispensabile sia per la valutazione del rischio, che per agevolare la supervisione del Garante. La tenuta del registro è obbligatoria per tutti i titolari e i responsabili con più di 250 dipendenti. Sotto tale soglia, invece, l'obbligo sussiste solo per il *controller* che effettui trattamenti cd. a rischio (art. 30, par. 5, del GDPR). Inoltre, il registro deve riportare le informazioni di cui all'art. 30, parr.1 e 2, del GDPR ed avere forma scritta, anche elettronica. Sul punto, cfr. anche il contributo del Garante per la protezione dei dati personali, Accountability *(responsabilizzazione). Approccio basato sul rischio e misure di* accountability*(responsabilizzazione) di titolari e responsabili*, disponibile *online* su https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di accountability-responsabilizzazione-di-titolari-e-responsabili.

[144] Così L. Greco, *op. ult. cit.,* pp. 279 e ss.

Capitolo II

La responsabilità da trattamento illecito dei dati personali

Sommario: 1. Il nuovo approccio del GDPR fra recessività dell'autodeterminazione e centralità del rischio; 1.1. Il *risked based approach* ; 1.2. L'autoregolamentazione nel GDPR: numerosi gli strumenti contemplati dal Regolamento; 1.2.1. Certificazioni e codici di condotta come "*Accountability Tools*"; 2. Dalla responsabilizzazione alla responsabilità degli attori del trattamento; 2.1. La responsabilità *ex* art. 23 della Direttiva 95/46 CE e la sua attuazione nella legislazione italiana; 2.1.1. Cenni sull'attuazione della responsabilità *ex* art. 23 della Direttiva 95/46 CE nelle legislazioni europee; 3. La responsabilità *ex* art. 82 GDPR: gli elementi costitutivi della fattispecie; 3.1. La responsabilità per illecito trattamento dei dati. Una natura giuridica controversa; 3.2. La responsabilità *ex* art. 82 GDPR, una responsabilità autonoma e speciale; 3.2.1. Uno sguardo alla giurisprudenza europea sul danno immateriale; 3.2.2. Le criticità della responsabilità *ex* art. 82 GDPR al vaglio della Corte di Giustizia: il caso UI contro *Österreichische Post AG;* 4. La responsabilità solidale degli attori del trattamento; 4.1. Titolarità congiunta del trattamento e responsabilità solidale; 4.2. I soggetti esonerati dal regime di responsabilità solidale

1. Il nuovo approccio del GDPR fra recessività dell'autodeterminazione e centralità del rischio

Sin dal 1978, il legislatore europeo si è focalizzato sulla regolazione del rapporto fra il principio della libera circolazione dei dati e il diritto dei singoli di disporre dei propri dati[145]. Tale diritto, nel tempo, aveva acquisito lo *status* di libertà fondamentale, circostanza che aveva determinato il sorgere di un ulteriore diritto in capo al *data subject*: essere informato sul trattamento di dati a lui riconducibili e potervi acconsentire o meno. Il consenso dell'interessato assumeva così un ruolo centrale per il trattamento dei dati, tanto da aggiungersi alle altre condizioni di

[145]Il binomio "libera circolazione dei dati all'interno dell'Unione" e "tutela della persona" rappresenta ancora oggi il fulcro della normativa in materia di protezione dei dati, tanto da costituire l'oggetto di tutela del GDPR. Ciò, emerge sia dall'art. 1, par. 1, del GDPR, sia dai considerando nn. 6, 13 e 170.

liceità previste *ex lege*, quale l'interesse pubblico e la tutela dei diritti fondamentali del *data subject.* Tuttavia, perché l'assenso dell'interessato potesse costituire la base giuridica del trattamento, il legislatore dell'epoca, come quello attuale, aveva stabilito che ad esso dovesse corrispondesse un'autodeterminazione libera e informata. La previsione di un simile requisito non stupisce, se associata a ciò che stava avvenendo in quegli anni nel contesto dottrinale e giurisprudenziale italiano. Tramite una lettura evolutiva della Costituzione, veniva superata la concezione dei diritti fondamentali come "numero chiuso", essendo a questa preferita l'idea che tali diritti costituiscono un novero ampliabile in base alle esigenze della società. D'altronde, i nuovi diritti rinverrebbero il proprio fondamento costituzionale nell'art. 2 della Carta, il quale, essendo una clausola "aperta", ne favorisce l'enucleazione[146]. In virtù di tali considerazioni, la dottrina riconosceva anche al diritto di autodeterminazione, inteso come diritto al <<riconoscimento della capacità di scelta autonoma ed indipendente dell'individuo>>[147], natura di diritto costituzionalmente protetto.

Benché trovasse fondamento nella Costituzione, e fosse un requisito imprescindibile del consenso dell'interessato, con l'evoluzione tecnologica il diritto di autodeterminazione perse la sua centralità nel trattamento dei dati. Del resto, in una società improntata alla digitalizzazione, era inevitabile che ciò avvenisse, considerando che all'aumentare dei trattamenti di dati, diminuiva anche l'attenzione da parte degli interessati nell'autorizzarli[148]. Consapevole di questi limiti, nel Regolamento il legislatore ha adottato un approccio differente, prevedendo: da un lato, ipotesi in cui l'interesse del singolo ad autorizzare il trattamento soccombe, *ex lege*, rispetto ad altri interessi; dall'altro, fattispecie ove è possibile ricorrere a basi giuridiche del trattamento diverse dal consenso del *data subject.*

---

[146]Sul fondamento costituzionale del diritto di autodeterminazione, v. A. De Vita, *Il diritto all'autodeterminazione in ambito sanitario e il testamento biologico: verso nuove frontiere del diritto? Il diritto della sanità: problematiche attuali**, 2020, disponibile *online* su https://www.giustizia-amministrativa.it/-/de-vita-il-diritto-all-autodeterminazione-in-ambito-sanitario-e-il-testamento-biologico-verso-nuove-frontiere-del-diritto-il-diritto-della-sanita-prob.

[147]S. Mangiameli, relazione tenuta al IV Laboratorio Sublacense su "La comunità familiare e le scelte di fine vita" del 3-5 luglio 2009, dal titolo <<*Autodeterminazione: diritto di spessore costituzionale*>>, p. 1, disponibile *online* su https://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0148_mangiameli.pdf.

[148]Per un'analisi approfondita sul consenso dell'interessato al trattamento dei dati, v. I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio del diritto civile e commerciale*, 2018, n. 1, pp. 67 e ss.

Quanto al primo caso, si fa riferimento alle operazioni che fuoriescono dall'ambito di applicazione del GDPR[149], giacché in queste situazioni sussistono interessi prevalenti rispetto a quelli del singolo. Tali operazioni sono individuate all'art. 2, par. 2, del GDPR, il quale prevede che non sono soggetti alle disposizioni del Regolamento i trattamenti:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

La prima fattispecie, sebbene non sia di facile interpretazione, sembra alludere a situazioni in cui il trattamento dei dati sia giustificato da esigenze di sicurezza nazionale, che prevalgono sul consenso del *data subject* e impediscono ogni opposizione al trattamento[150]. Quanto al secondo punto, dato il riferimento al titolo V, capo 2, del Trattato sull'Unione Europea, esso si riferisce ai trattamenti realizzati dagli Stati membri per ragioni di politica estera, sicurezza e difesa comune. Ancora una volta, è la *national security* a predominare sulla *data protection*. Per quel che attiene la terza casistica, ossia i trattamenti effettuati da una persona fisica per attività personali o domestiche, il GDPR si limita a riportare quanto già previsto dalla Direttiva; pertanto, il Regolamento non interviene a colmare i dubbi sugli elementi che differenziano il carattere personale da quello domestico[151]. Infine, sono esclusi dal campo di applicazione del GDPR i trattamenti

[149]L'ambito di applicazione materiale del Regolamento è definito dall'art. 2 GDPR, che, al primo paragrafo, ne circoscrive l'applicabilità al trattamento, automatizzato o manuale, di dati personali che siano archiviati o destinati a essere inclusi in un archivio.

[150]In dottrina si discute dell'esistenza di un limite alla prevalenza delle esigenze di sicurezza nazionale rispetto alla protezione dei diritti e delle libertà individuali, incluso il diritto alla privacy: *ex multis,* v. S. Sica, G. Giannone Codiglione*, La libertà fragile. Pubblico e privato al tempo della rete*, Napoli, Edizioni Scientifiche Italiane, 2014, pp. 25 e ss.; F. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*., vol. XLVIII, 2007, pp. 609 e ss.

[151]Il GDPR fornisce qualche ulteriore elemento interpretativo al considerando n. 18, il quale stabilisce che <<il presente regolamento non si applica al trattamento di dati personali effettuato da

volti a perseguire l'interesse pubblico della lotta alla criminalità e della sicurezza nazionale, dovendo essere valutata caso per caso l'effettiva esistenza di detto interesse[152].

Oltre alle summenzionate ipotesi, il GDPR ammette che possa prescindersi dal consenso dell'interessato allorché ricorrano condizioni di liceità differenti; ciò vale tanto per il trattamento di dati personali comuni, quanto per quelli sensibili [153] e quelli giudiziari penali. In relazione a queste ultime tipologie di dati, però, il ricorso a basi giuridiche alternative incontra dei limiti. Invero, i dati giudiziari penali possono essere trattati solo previa autorizzazione di legge, o sotto il controllo della pubblica autorità[154]. Quanto ai dati sensibili, è vietato disporne, salvo che non sussista il consenso espresso dell'interessato, oppure una delle condizioni di cui all'art. 9 del GDPR[155].

Fra le basi giuridiche alternative, il Regolamento annovera, *in primis*, l'esecuzione di un contratto o di misure precontrattuali; eppure, nel contemplarla, il GDPR adotta una formulazione che sembra discostarsi dalla tradizione giuridica di *civil law*, in quanto riduce l'applicazione della base in esame ai soli casi in cui l'interessato sia <<parte del contratto>>. Malgrado l'art. 6, lett. b, del GDPR si

---

una per sona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico>>.

[152]Cfr. R. Torino, *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679,* in *La cittadinanza europea,* 2018, n. 2, pp. 50 e ss.

[153]Con l'espressione dati sensibili si fa riferimento a quella particolare tipologia di dati relativa a: razza o etnia, convinzioni religiose e filosofiche, opinioni politiche, appartenenza sindacale, salute e vita sessuale. Inoltre, ai sensi dell'art. 9 del GDPR, appartengono alla categoria in esame anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale. Per ulteriori chiarimenti in merito alla classificazione dei dati personali, v. il Garante per la protezione dei dati personali, *Cosa intendiamo per dati personali? *,* disponibile *online* su https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali.

[154]Le suddette condizioni di liceità sono previste dall'art. 10 GDPR.

[155]Ai sensi dell'art. 9, par. 2, del GDPR il divieto di trattare i dati sensibili viene meno quando l'interessato abbia acconsentito esplicitamente al trattamento di tali dati per ragioni precise; il trattamento sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; il trattamento riguardi dati personali che l'interessato abbia contribuito a rendere pubblici; il trattamento sia diretto ad uno dei seguenti scopi: conformarsi agli obblighi del *controller* o del *data subject* in materia di diritto del lavoro e della sicurezza sociale; salvaguardare un interesse vitale del *data subject* o di un soggetto terzo, qualora il primo sia incapace di prestare il proprio consenso; azionare o tutelare un diritto in sede giudiziaria. Ancora, il trattamento è consentito allorché sia necessario per ragioni di: interesse pubblico ritenute rilevanti dal diritto dell'Unione o degli Stati membri; medicina preventiva o del lavoro ecc.; interesse pubblico nel settore della sanità pubblica; archiviazione nel pubblico interesse, ricerca scientifica, storica e statistica.

riferisca esclusivamente alle parti, ovvero ai soggetti che intervengono nella stipula, la norma appare altrettanto applicabile alle ipotesi di successione nel rapporto contrattuale, sia a titolo particolare, ai sensi degli artt. 1406 c.c. e 2558 c.c., che universale, come previsto dall'art. 456 c.c. e seguenti. Maggiori perplessità sorgono, invece, rispetto alla possibilità di estendere la previsione del GDPR alla parte di un atto giuridico non contrattuale, nonché alla persona fisica che subentri solamente nel lato attivo o passivo dell'obbligazione, e non nella posizione contrattuale *in toto*. (art. 1260 c.c., artt. 1235, 1268 e ss. c.c.). I medesimi dubbi si ripropongono nei confronti dei soggetti che, pur non essendo parti formali del contratto, risultano esserne i beneficiari (art. 1411 c.c)., o co-obbligati (art. 1292 c.c.). Benché l'art. 6, lett. b, non sia di immediata applicazione, l'interpretazione teleologica della disposizione sembra consentire il trattamento anche nelle fattispecie appena descritte[156].

Altrettanto problematica appare l'ultima condizione di liceità di cui all'art. 6 GDPR, vale a dire <<il perseguimento del legittimo interesse del titolare del trattamento o di terzi>>. I dubbi su questa base giuridica derivano dalla sua formulazione, poiché si richiama un concetto "indeterminato", quale quello di interesse legittimo, e si stabilisce la necessità di un bilanciamento fra l'interesse del titolare e il consenso dell'interessato[157]. Rispetto a tale operazione, il legislatore si limita ad indicare i criteri per eseguire il *balancing test,* il quale non è più una prerogativa del Garante per la protezione dei dati, ma, in un'ottica di *accountability*, è rimesso al titolare[158]. Pur essendo una norma "aperta", la condizione di cui alla lett. f non deve rappresentare una "scappatoia" della quale il *controller* si serve per eludere la normativa sulla *data protection*; allo stesso tempo, essa non deve neppure essere interpretata in maniera così rigida da ridurne al minimo l'operatività[159].

---

[156] In questo senso, v. A. Fedi, *Diritto dell'impresa e protezione dei dati personali*, in *Società*, 2018, n. 10, pp. 1095 e ss.

[157]L'art. 6, lett. f, del GDPR precisa che l'interesse legittimo del titolare costituisce la base giuridica del trattamento <<a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore>>.

[158] Sull'interesse legittimo come base giuridica alternativa del trattamento, v. D. Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza Italiana*, 2019, n. 12, pp. 2787 e ss.

[159]Sulla necessità di evitare le due estremizzazioni, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE* (WP 217), 9 aprile 2014, parr. 1 e 2.4, disponibile *online* su https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

Proprio per evitare ciò, il Regolamento fornisce al titolare degli esempi di trattamento ove il legittimo interesse del *controller* è da ritenersi prevalente[160].

Accanto alle basi giuridiche di più incerta interpretazione, il legislatore europeo ha considerato altresì legittimo il trattamento dei dati realizzato per attendere ad un obbligo legale del titolare, nonché per tutelare gli interessi vitali di una persona fisica, come i diritti previsti dalla Carta di Nizza; ed ancora, per eseguire compiti di interesse pubblico o legati all'esercizio di pubblici poteri[161]. Ebbene, se è vero che in dette ipotesi il consenso dell'interessato tende a soccombere, è pur vero che, nel caso in cui sussistano ragioni di interesse pubblico, il *data subject* conserva, in parte, il suo diritto all'autodeterminazione, potendo opporsi al trattamento che il titolare ha avviato senza il suo consenso. Allo stesso modo, l'interessato può manifestare la sua opposizione anche quando il trattamento sia necessario per il perseguimento del legittimo interesse del titolare o di terzi[162]. Al pari della Direttiva, quindi, il GDPR prevede la facoltà di opposizione dell'interessato; tuttavia, se ne discosta laddove pone dei limiti al suo esercizio. Difatti, il legislatore ha rimosso dall'art. 21 del GDPR l'espressione "almeno", la quale precedeva l'enunciazione dei casi dell'interesse pubblico e dell'interesse legittimo nella Direttiva[163]; così facendo, ha finito per riconoscere il diritto di opposizione in relazione a queste due uniche fattispecie, salvo l'eccezione del trattamento per finalità di *marketing* diretto[164] di cui all'art. 21, par. 2, del GDPR.

---

[160]Le esemplificazioni coprono una vasta area di interessi che va da quello alla prevenzione delle frodi a quello di *marketing* diretto (considerando n. 47); dall'interesse alla condivisione di dati tra soggetti dello stesso gruppo di impresa per ragioni amministrative (considerando n. 48) al trattamento di dati personali relativi al traffico, nella misura indispensabile per assicurare la tutela delle reti e dell'informazione (considerando n. 49).

[161]Le succitate condizioni di liceità sono contemplate, rispettivamente, alle lett. c, d ed e dell'art. 6 GDPR.

[162]L'art. 21, par. 1, del GDPR statuisce che <<l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni>>.

[163]La Direttiva 95/46 CE, all'art. 14, par. 1, stabiliva che <<gli Stati membri riconoscono alla persona interessata il diritto: a) almeno nei casi di cui all'articolo 7, lettere e) e f) [ragioni di interesse pubblico e perseguimento del legittimo interesse del titolare o di terzi], di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale>>.

[164]Il Regolamento non fornisce una definizione di "*marketing* diretto"; tuttavia, nella prassi economico-aziendale, tale espressione viene utilizzata per riferirsi a <<*the communication (by whatever means) of advertising or marketing material which is directed to particular individuals*>> (così Information Commissioner's Office, *Direct marketing detailed guidance*, 5 dicembre 2022, p. 10, disponibile *online* su https://ico.org.uk/media/for-organisations/direct-marketing-guidance-and-resources/direct-marketing-guidance-1-0.pdf.) In argomento, v. S. Stabile, *Le nuove frontiere della pubblicità e del* marketing *su internet*, in *Diritto Industriale*, 2009, n. 5, pp. 482 e ss.

Inoltre, il GDPR consente al *controller* di continuare a utilizzare i dati dell'interessato anche in caso di opposizione, purché provi che le ragioni per proseguire siano prevalenti rispetto ai diritti e le libertà del *data subject;* oppure, che il trattamento sia finalizzato ad accertare, esercitare o difendere un diritto in sede giudiziaria[165].

Dalla differente regolazione del consenso, emerge chiaramente il cambio di prospettiva avvenuto nel GDPR. Il legislatore europeo, infatti, ha ritenuto che l'obiettivo di tutela dei dati personali non fosse perseguibile mediante il solo riconoscimento di diritti in capo all'interessato, il quale non sempre è in grado di esercitarli scientemente. Pertanto, egli ha ritenuto più opportuno implementare gli oneri del *processor* e del *controller.* D'altronde, come si è già osservato, il Regolamento pone in capo al *controller* l'obbligo di adottare misure preventive, quali: la valutazione di impatto (artt. 35 e ss. GDPR); la progettazione per impostazione predefinita di sistemi che riducano al minimo l'utilizzo di dati personali *(*art. 25 GDPR); la nomina di un soggetto terzo che assicuri la corretta gestione dei dati presso aziende ed enti, ovvero il *Data Protection Officer* o responsabile della protezione dei dati personali *(*artt. 37 e ss. GDPR)*[166]*. Ognuna di queste misure è volta a responsabilizzare il titolare tramite l'adozione di procedure che eliminino, o quanto meno riducano, i rischi per i dati trattati[167].

Dunque, appare evidente che alla precedente concezione del trattamento dei dati come attività pericolosa tutelata *ex post*, il GDPR ha preferito un'impostazione di tutela *ex ante* di prevenzione del danno. In ragione di ciò, l'analisi e la gestione del rischio derivante dall'attività di trattamento, insieme alla responsabilizzazione del titolare, divengono i pilastri del nuovo impianto normativo[168].

---

[165]Sulla regolazione del diritto di opposizione dell'interessato nel GDPR, v. D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda* "Cambridge Analytica", in *federalismi.it,* 2018, n. 20, pp. 13 e ss.

[166] Il *Data Protection Officer* (DPO) è una figura istituita dal Regolamento, il quale disciplina il DPO agli artt. 37 – 39 GDPR. In via generale, tale soggetto è incaricato di promuovere la cultura della *data protection* presso l'organizzazione del *controller* o del *processor*; a tal fine, questi può esercitare funzioni consultive, decisorie e preventive. Per un'analisi approfondita sul DPO, v. A. Avitabile, *Il* Data Protection Officer, in G. Finocchiaro (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* cit., pp. 331 e ss.

[167]Sugli obblighi di natura preventiva del titolare del trattamento, v. I. A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale,* in *Annali-Università degli Studi Suor Orsola Benincasa,* vol. XI, 2021, n. 1, pp. 16 e ss.

[168]Cfr. E. Tosi, *Diritto privato delle nuove tecnologie digitali. Riservatezza, contratti, responsabilità fra persona e mercato,* in V. Franceschelli, E. Tosi (diretto da), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2021, pp. 568 e ss.

1.1. Il *risked based approach*

Nel GDPR assume un ruolo fondamentale il concetto di rischio, dovendo con tale termine intendersi uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità[169]. Siffatta rilevanza ha una duplice giustificazione: da un lato, il rischio rappresenta uno dei criteri che il *controller* deve valutare nella scelta delle misure tecniche e organizzative più adeguate; dall'altro, è il rischio a fa sorgere l'obbligo per il titolare di adottare tali misure, le quali altrimenti non sarebbero necessarie. Non stupisce che il rischio abbia un'importanza simile nel Regolamento; al contrario, la sua centralità è in linea con l'approccio adottato dal legislatore europeo, il quale, attraverso il GDPR, mira a una protezione dei dati più proattiva, modulabile ed efficace[170]. Questi obiettivi sono perseguiti tramite il "*risked based approach*", che, come anticipato, impone ai titolari di scegliere le misure appropriate a garantire la sicurezza dei dati, considerando i rischi che possano derivare dalle attività di trattamento. Tale approccio si evince principalmente dagli artt. 24 e 25 del GDPR. In particolare, il primo, enunciando il principio di *accountability,* impone al *controller* di adottare le misure necessarie a conformarsi al GDPR, tenendo conto del rischio per i diritti delle persone fisiche; infatti, solo adottando misure proporzionate al rischio, il titolare può dimostrare la conformità al Regolamento. Il secondo, invece, richiede al *controller* di proteggere i dati fin dalla progettazione, considerando, ancora una volta, i rischi per le facoltà e le libertà dei soggetti coinvolti nel trattamento. Questi articoli formulano il "*risked based approach*", in quanto spostano l'attenzione dalla mera conformità legale a misure proattive e preventive, capaci di ridurre i potenziali rischi per gli interessati.

Passando alle caratteristiche del suddetto approccio, esso è "modulabile", vale a dire che l'estensione delle misure dipende dal livello di rischio rilevato: i

---

[169]In questi termini, Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev.01), 4 aprile 2017, par. 3, disponibile *online* su https://ec.europa.eu/newsroom/article29/items/611236/en. In modo analogo, il Regolamento, ai considerando nn. 75 e 76, menziona la gravità e la probabilità come criteri di valutazione del rischio.

[170]Sul senso del "rischio" e del "*risked based approach*" nel GDPR, v. K. Demetzou, *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, in E. Kosta et al. (a cura di), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Berlino, Springer, 2019, pp. 137 e ss.

trattamenti a basso rischio richiedono meno precauzioni, mentre le attività ad alto rischio necessitano di misure di salvaguardia più rigorose[171]. Oltretutto, la modulabilità è intrinsecamente connessa al principio di *accountability*, in quanto esso è attuato attraverso obblighi modulabili, il cui rispetto determina la conformità al GDPR da parte del titolare[172].

Alla luce di tali considerazioni, emerge come il "*risked based approach*" abbia modificato il senso di "conformità al GDPR", poiché richiede ai titolari non solo di rispettare le norme, ma anche di interpretarle e applicarle in modo da proteggere effettivamente i diritti degli interessati. Così facendo, l'approccio si allontana da una mentalità di "spunta delle caselle" e si avvicina a una conformità sostanziale, che affronta l'impatto reale dell'attività di trattamento dei dati. In sintesi, il "*risked based approach*" è un pilastro del quadro normativo del GDPR, giacché enfatizza la responsabilizzazione e la gestione proattiva dei rischi. Esso richiede al *controller* di valutare e affrontare i rischi per i *data subject*, garantendo che la protezione dei dati sia parte integrante delle sue operazioni e dei processi decisionali[173] .

Nell'ambito del rapporto tra "*risked based approach*" e principio di *accountability*, si inserisce un altro elemento, ossia quello dell'autoregolamentazione privata. Quest'ultima, infatti, non solo consente una maggiore elasticità nella gestione del rischio derivante dal trattamento, ma agevola anche il titolare nel dimostrare la *compliance* ai propri obblighi, nonché il responsabile nell'attestare di avere tutte le garanzie richieste dal Regolamento; ciò, grazie agli "*accountability tools*": codici di condotta e certificazioni[174].

---

[171]Per alcune riflessioni in merito al carattere modulabile delle misure di conformità al GDPR, v. il Garante europeo per la protezione dei dati, *Opinion on coherent enforcement of fundamental rights in the age of big data*, 23 settembre 2016, par. 2.1., disponibile *online* su https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf, il quale afferma che <<*Obligations […] are scalable: where a company, for example, enjoys greater market power (a concern for competition authorities), or a stronger contractual position (consumer protection), or is responsible for riskier data processing operations (data protection), they are required to be more diligent in the steps they take to comply*>>.

[172] Cfr. K. Demetzou, *GDPR and the Concept of Risk,* cit., p. 142 e ss.

[173]Così C. Quellea, *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk Based Approach*, in *European Journal of Risk Regulation*, vol. IX, 2018, n. 3, pp. 2 e ss.

[174]Sul rapporto tra principio di *accountability* e autoregolamentazione privata, v. D. Poletti, M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), *Privacy Digitale,* cit., pp. 378 e ss.

1.2. L'autoregolamentazione nel GDPR: numerosi gli strumenti contemplati dal Regolamento

L'autoregolamentazione è un concetto ampio che comprende una vasta gamma di strumenti, quali codici di condotta, standard tecnici, certificazioni, sigilli e marchi. Il termine stesso è riconducibile a una pluralità di definizioni; tuttavia, volendo descriverlo in maniera negativa, l'autoregolamentazione è "non legislativa". Difatti, le leggi sono varate con procedure specifiche, che richiedono il coinvolgimento delle autorità statali, e sono applicabili all'intera popolazione, caratteristiche che non si riscontrano negli strumenti di autoregolamentazione.

Nel tentativo di definire l'autoregolamentazione, parte della dottrina ha operato un confronto con i concetti di deregolamentazione e non-regolamentazione. Quanto al primo, la deregolamentazione mira a rimuovere qualsiasi regolamento che tenda ad ostacolare le forze di mercato. Al contrario, l'autoregolamentazione non cerca di eliminare il quadro normativo che regola l'attività privata, ma piuttosto di modificare l'attore che stabilisce tale quadro. Quanto al secondo concetto, l'autoregolamentazione si discosta anche da questo, poiché, a differenza della non regolamentazione, essa non rappresenta un'alternativa o un sostituto per elementi di regolamentazione diretta[175].

Non rilevando elementi comuni con nessuno dei due termini, la dottrina in esame ha quindi analizzato le componenti dell'autoregolamentazione: "auto" e "regolamentazione". Ebbene, il prefisso "auto" si riferisce a un'associazione di persone, o di enti, che agiscono insieme; questi, in qualità di gruppo collettivo, non regolano solo sé stessi, bensì ogni altra persona o entità che accetti la loro autorità. Il termine "regolamentazione", invece, si riferisce alla capacità normativa del gruppo o dell'entità autoregolatoria. Dunque, l'espressione autoregolamentazione si riferisce a un insieme di persone, fisiche o giuridiche, che esercitano una funzione regolatoria su di sé e su chiunque riconosca loro tale potestà[176].

---

[175] Così M. Price, S. Verhulst, *The Concept of Self-Regulation and the Internet*, in J. Waltermann, M. Machill (a cura di), *Protecting our children on the internet: Towards a new culture of responsibility*, Gütersloh, Bertelsmann Foundation Publishers, 2000, pp. 133 e ss, i quali oltre a sostenere che <<*self-regulation is different from de-regulation or non-regulation*>>, ritengono che << *there is no single definition of self-regulation that is entirely satisfactory, nor should there be. Self-regulation evolves as the nature of the Internet alters*>>.

[176] Sul significato del termine "autoregolamentazione", v. J. Black, *Constitutionalising self-regulation*, in *The Modern Law Review*, vol. LIX, 1996, n. 1, pp. 24 e ss.

Rispetto alla regolamentazione per via legislativa, è indubbio che l'autoregolamentazione presenta dei vantaggi, fra i quali non possono non menzionarsi la flessibilità e l'adattabilità alle nuove esigenze tecnologiche. Inoltre, l'autoregolamentazione è orientata al consumatore, perché gli permette di avere delle risposte rapide sulle questioni relative alla privacy[177]. Ancora, l'autoregolamentazione coinvolge gli attori del mercato nella redazione dei suoi strumenti regolatori; pertanto, questi sono più propensi ad adottarli.

Oltre ai numerosi benefici, l'autoregolamentazione potrebbe comportare anche un notevole svantaggio, potendo incidere negativamente sia sui consumatori, che sugli *stakeholder* (in particolare, le piccole e medie imprese); invero, i loro diritti potrebbero non essere sufficientemente protetti dalle iniziative autoregolatorie guidate dalla grande industria[178].

Le certificazioni

Relativamente alle modalità di attuazione dell'autoregolamentazione, essa viene implementata tramite una varietà di mezzi: il GDPR riconosce sia i codici di condotta, che altre forme di autoregolamentazione, come la standardizzazione e le certificazioni[179]. Con riferimento a quest'ultimo strumento, il Regolamento lo formalizza mediante due articoli, il 42 e il 43, i quali inquadrano la progettazione e il funzionamento degli schemi di certificazione nell'ambito della protezione dei dati. Secondo tali norme, qualsiasi organismo può impostare uno schema di certificazione e sottoporre i requisiti di certificazione all'approvazione dell'autorità di controllo competente, o al Comitato europeo per la protezione dei dati (quando l'organismo intenda dare una copertura transfrontaliera allo schema).Tuttavia, perché possa valutare la conformità di un candidato e, qualora la valutazione abbia

[177]Cfr. N. Doty, D. K. Mulligan, *Internet Multistakeholder Processes and Techno—Policy Standards. Initial Reflections on Privacy at the World Wide Web Consortium*, in *Journal on Telecommunications & High Technology Law*, 2013, n. 11, pp. 138 e ss.

[178]Circa i vantaggi e gli svantaggi che derivano dall'autoregolamentazione, v. I. Kamara, *Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation mandate*, in *European Journal of Law and Technology*, vol. VIII, 2017, n. 1, pp. 4 e ss.

[179]La regolazione di tali strumenti da parte del GDPR è la prova che il legislatore europeo considera l'autoregolamentazione un supporto alla normativa dell'Unione.

esito positivo, rilasciare la certificazione, l'organismo deve essere accreditato secondo uno dei processi previsti dall'art. 43, par. 1, del GDPR[180].

Gli organismi accreditati non sono i soli a poter emettere certificazioni: le autorità nazionali di controllo sono autorizzate a istituire meccanismi di certificazione secondo il regime degli artt. 42 e 43 GDPR[181]. Diversamente dagli organismi, le autorità di controllo non sono tenute ad essere accreditate. Malgrado ciò, l'EDPB ha raccomandato alle autorità di controllo di adottare misure organizzative adeguate a separare i compiti previsti dal GDPR, così da consolidare e facilitare i meccanismi di certificazione; ed altresì di prendere precauzioni per evitare eventuali conflitti di interesse che possano sorgere da tali compiti[182].

In materia di certificazioni, quello appena descritto non è stato l'unico intervento del Comitato europeo per la protezione dei dati. L'EDPB ha dovuto ovviare ad una grande mancanza del GDPR, quale l'assenza di una definizione chiara e precisa di certificazione. A tal fine, il Comitato si è ispirato alla definizione generale di certificazione dell'Organizzazione internazionale per la normazione (ISO), secondo cui la certificazione è la fornitura, da parte di un organismo indipendente, di un'assicurazione scritta (un certificato) che il prodotto, servizio o sistema in questione soddisfa specifici criteri[183]; quindi, ne ha elaborata una propria. A parere del Comitato, per certificazione si intende la valutazione e l'attestazione imparziale, da parte di un soggetto terzo, che i criteri di certificazione sono stati rispettati[184].

Con tale definizione, l'EDPB riconosce alla certificazione natura sia di valutazione, che di attestazione di conformità. Eppure, il sistema di certificazione

---

[180]Il Comitato Europeo per la Protezione dei Dati, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* 4 giugno 2019, par. 3.28, disponibile *online* su https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf, definisce l'accreditamento come l'attestazione, da parte di un organismo nazionale di accreditamento e/o da parte di un'autorità di controllo, che un organismo è qualificato per eseguire certificazioni ai sensi degli artt. 42 e 43 del GDPR, tenendo conto della norma ISO/IEC 17065/2012 e dei requisiti aggiuntivi stabiliti dall'autorità di controllo e/o dal Comitato.

[181]Il rilascio di certificazioni da parte delle autorità di controllo competenti è disciplinato dall'art. 42, par. 5, GDPR.

[182]Il Comitato Europeo per la Protezione dei Dati, *op. ult. cit*., par. 4.5.

[183]Così l'Organizzazione internazionale per la normazione (ISO), *Certification*, disponibile *online* su https://www.iso.org/certification.html.

[184]In questi termini, il Comitato Europeo per la Protezione dei Dati, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679),* cit., par. 2.

descritto dal Regolamento è leggermente diverso, poiché non solo include ulteriori caratteristiche rispetto a quelle previste dal Comitato, ma soddisfa obiettivi che vanno oltre l'attestazione di conformità ai requisiti di certificazione. Prima di tutto, la certificazione, per come disciplinata dal GDPR, include il riconoscimento dei requisiti di certificazione da parte degli organismi competenti, nonché l'accreditamento di questi ultimi, salvo si tratti di autorità di controllo. In secondo luogo, la certificazione del Regolamento presente delle caratteristiche estranee alla definizione del Comitato. Fra queste, vi sono la validità limitata nel tempo, in quanto la certificazione ha una durata massima di tre anni, e la sua rinnovabilità mediante la medesima procedura del rilascio. Inoltre, la certificazione è "condizionata", poiché l'autorità di controllo è autorizzata a negarla allorchè non siano soddisfatti tutti i requisiti del GDPR. Al pari del rilascio, anche il mantenimento e il rinnovo della certificazione sono subordinati alla conservazione della conformità durante il periodo di validità. Difatti, la certificazione può essere revocata in qualsiasi momento dall'organismo o dall'autorità di controllo, qualora le condizioni di rilascio non siano più soddisfatte.

Oltre ad omettere alcuni dei requisiti richiesti dal GDPR per la certificazione, l'EDPB, nella sua definizione, non fa neppure riferimento all'ulteriore scopo per cui il Regolamento prevede questa forma di autoregolamentazione. La certificazione, infatti, non si limita ad attestare la conformità alla normativa sulla *data protection*, ma è stata introdotta dal legislatore europeo come strumento di responsabilizzazione. Del resto, la certificazione permette a *controller* e *processor* di dimostrare, almeno formalmente, l'osservanza del GDPR, garantendo così una sorta di "presunzione di conformità"[185].

I codici di condotta

Il Regolamento introduce disposizioni più dettagliate sui codici di condotta rispetto a quelle presenti nella Direttiva 95/46 CE. Quest'ultima si riferiva ai codici in termini generali, attribuendo agli Stati membri e alla Commissione il compito di incoraggiare le associazioni professionali, nonché gli organismi rappresentativi di altre categorie di titolari, a sviluppare codici di condotta (art. 27, par. 1). Detti

[185]Per approfondimenti sui meccanismi di certificazione nel GDPR, v. E. Lachaud, *What GDPR tells about certification*, in Computer Law & Security Review, 2020, n. 38, pp. 7 e ss.

strumenti contribuivano alla corretta applicazione della legislazione sulla protezione dei dati, giacché tenevano conto delle caratteristiche specifiche dei vari settori. La Direttiva, però, non contemplava un'unica tipologia di codici, ma distingueva i codici nazionali da quelli comunitari. In virtù di tale distinzione, un progetto di codice di condotta nazionale, come pure una proposta di modifica o proroga di un codice esistente, doveva essere sottoposto al vaglio dell'autorità di controllo nazionale, la quale era chiamata a valutare se il progetto fosse conforme alla legislazione statale che attuava la Direttiva (art. 27, par. 2). Per quel che atteneva il codice di condotta comunitario, invece, il parere di valutazione era di competenza del Gruppo di lavoro per la protezione dei dati personali (Art. 29). A seguito di tale parere, interveniva la Commissione Europea, che aveva il compito di garantire l'adeguata pubblicizzazione dei codici comunitari approvati (art. 27, par. 3).

Malgrado la Direttiva disciplinasse i codici di condotta, le sue disposizioni avevano trovato scarsa applicazione in concreto[186]; difatti, durante la sua vigenza, era stato approvato solo un limitato numero di codici[187]. Tale esiguità era riconducibile a una pluralità di fattori: da una parte, la lunghezza dei tempi di approvazione dei codici, spesso dovuta, per quanto riguarda i codici comunitari, alla minuziosità dell'analisi del Gruppo di lavoro. Dall'altra, l'art. 27, par. 3, della Direttiva richiedeva che i codici comunitari fossero conformi alle leggi nazionali sulla *data protection*[188]. Dunque, perché fossero approvati, non era sufficiente che i codici fossero conformi alla Direttiva, ma occorreva che osservassero i requisiti legali di ciascuno Stato Membro[189].

---

[186]Cfr. Commissione Europea, *Un approccio globale alla protezione dei dati personali nell'Unione Europea,* cit., par. *2.2.5.,* la quale affermava che <<finora [erano] state raramente applicate le disposizioni della direttiva sulla protezione dei dati relative all'autoregolamentazione, ovvero all'elaborazione di codici di condotta, ritenute insoddisfacenti dalle parti interessate>>.

[187]Nel 2003, il Gruppo di lavoro per la protezione dei dati personali (Art. 29) ha valutato positivamente il codice comunitario di condotta sul *marketing* diretto presentato dalla Federazione Europea del *Direct Marketing* (FEDMA) (v. *Opinion on the European Code of conduct of FEDMA for the use of personal data in direct marketing* (WP 77), 13 giugno 2003, disponibile *online* su https://ec.europa.eu/newsroom/article29/items/667236/en).

[188]Sulle cause della scarsa diffusione dei codici di condotta, v. P. Drobek, *The role of codes of conduct in the EU data protection framework*, in *GIS Odyssey Journal*, vol. II, 2022, n. 2, pp. 132 e ss.

[189]Così C. Kuner, *European Data Protection Law. Corporate Compliance and Regulation*, Oxford, Oxford University Press, 2007, pp. 46 e ss., il quale riteneva che, per risolvere tali difficoltà, e promuovere l'adozione di codici di condotta a livello comunitario, il Gruppo di lavoro per la protezione dei dati personali dovesse cessare di insistere sull'applicazione di ogni norma di diritto nazionale in aggiunta a quelle previste dai codici di condotta.

Nel tentativo di rimediare al fallimento della Direttiva 95/46 CE, il Regolamento ha adottato un approccio differente nella regolazione dei codici di condotta, disciplinati agli artt. 40 e 41 del GDPR. *In primis*, è stato ampliato l'ambito soggettivo dei codici, i quali possono essere promossi da associazioni rappresentative non solo dei *controller*, bensì dei *processor*. Tale ampliamento non ha invece riguardato l'ambito oggettivo, essendo state indicate, seppur a titolo meramente esemplificativo, delle aree di regolamentazione[190]. Ancora, sono stati chiaramente definiti i ruoli degli attori coinvolti nella procedura, in particolare di: Stati membri, autorità di controllo nazionali, Comitato europeo per la protezione dei dati e Commissione Europea. Questi ultimi devono incoraggiare la corretta applicazione del GDPR, attraverso codici di condotta che tengano conto delle caratteristiche dei vari settori di trattamento, come pure delle esigenze delle piccole e medie imprese[191]. Sono state altresì precisate le questioni procedurali. Secondo il GDPR, il progetto di un codice di condotta, così come quello di modifica o proroga di codici vigenti, deve essere presentato all'autorità di controllo competente affinché questa possa emettere il parere di conformità al Regolamento e, qualora lo ritenga idoneo a fornire garanzie adeguate, approvarlo (art. 40, par. 5, GDPR). Nel caso in cui il progetto riguardi attività di trattamento che coinvolgano più Stati membri, l'autorità di controllo, prima di avvallarlo, deve sottoporre il progetto all'EDPB. Il Comitato è incaricato di esprimere un parere sulla conformità del progetto al GDPR, nonché sulla sua idoneità a offrire garanzie adeguate, quando questo abbia ad oggetto trasferimenti internazionali di dati (art. 40, par. 7, GDPR). Laddove il parere del Comitato sia favorevole, esso viene trasmesso alla

[190]Tra le aree potenzialmente disciplinabili con dei codici di condotta, il GDPR, all'art. 40, par. 2, elenca <<il trattamento corretto e trasparente dei dati; i legittimi interessi perseguiti dai [titolari del trattamento] in contesti specifici; la raccolta dei dati personali; la pseudonimizzazione dei dati personali; l'informazione fornita al pubblico e agli interessati; l'esercizio dei diritti degli interessati; l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore; le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32; la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni all'interessato; il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79>>.

[191] L'attività di promozione dei codici di condotta è rimessa ai suddetti soggetti ai sensi dell'art. 40, par. 2, GDPR.

Commissione, che può stabilire, mediante atti di esecuzione, la validità generale del codice di condotta all'interno dell'Unione (art. 40, par. 9, GDPR)[192].

Oltre a rivedere l*'iter* di approvazione dei codici di condotta, il legislatore europeo ha evidenziato l'urgenza di instaurare meccanismi di monitoraggio della *compliance.* Infatti, per ottemperare al principio di *accountability*, non è sufficiente che il *controller* o il *processor* aderiscano ad un codice di condotta, ma è necessario che questi ne diano concreta attuazione.

1.2.1. Certificazioni e codici di condotta come "*Accountability Tools*"

Benché l'adesione a codici di condotta e certificazioni non sia sufficiente, da sola, a garantire la conformità al principio di responsabilizzazione, è innegabile che contribuisca al perseguimento di tale obiettivo. Del resto, è lo stesso GDPR a riconoscere che, in numerose ipotesi, i suddetti strumenti costituiscono una "dimostrazione" del principio di *accountability,* intendendo quest'ultimo come la capacità di provare la conformità al Regolamento. Esemplificativo, in questo senso, è il caso del *processor*, che deve offrire al *controller* garanzie sufficienti sulla sua capacità di adottare misure tali da assicurare un trattamento rispettoso sia dei requisiti del GDPR, sia dei diritti dell'interessato. Ebbene, <<l'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti>>[193]. A sua volta, un sub-responsabile del trattamento, designato dal responsabile, può garantire al titolare l'attuazione di misure adeguate aderendo a codici di condotta e certificazioni[194].

Codici di condotta e certificazioni rivestono un ruolo altrettanto importante in materia di misure di sicurezza; difatti, l'adesione a tali strumenti attesta che *controller* e *processor* hanno scelto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (art. 32, par. 3, GDPR). La centralità dei codici di condotta emerge anche al momento di valutare l'impatto del

[192]Per attribuire validità generale al codice, la Commissione Europea deve attivare la "procedura di comitato" di cui all'art. 93, par. 2, GDPR, che, a sua volta, richiama la procedura d'esame di cui all'art. 5 del Regolamento (UE) n. 182 del 2011.
[193] Ai sensi dell'art. 28, par. 5, GDPR.
[194]Sull'osservanza dei codici di condotta da parte dei sub-responsabili del trattamento, v. C. Bistolfi, L. Bolognini, E. Pelino, *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali,* cit., pp. 430 e ss.

trattamento, giacché deve essere tenuto in considerazione se il titolare e il responsabile, nell'effettuarlo, abbiano rispettato i codici di condotta a cui avevano precedentemente aderito (art. 35, par. 8, GDPR). Infine, codici di condotta e certificazioni, assumono un ruolo fondamentale nell'applicazione delle sanzioni amministrative, poiché l'autorità competente, tra i vari aspetti, considera l'adesione a tali strumenti per determinare se, e in che misura, imporre una sanzione (art. 83, par. 2, lett. j, GDPR).

Da tale disamina, appare evidente che codici di condotta e certificazioni semplificano l'adempimento delle disposizioni del GDPR, in quanto chiariscono come ottemperare agli obblighi del Regolamento; inoltre, consolidano il principio di *accountability.* Invero, questi agevolano titolari e responsabili di settori specifici nell'applicazione della normativa, oltre a rendere le loro attività di trattamento più facilmente verificabili[195].

2. Dalla responsabilizzazione alla responsabilità degli attori del trattamento

Il principio di *accountability* riflette i propri effetti sulla responsabilità civile da trattamento illecito dei dati personali, arricchendola di significato. Nello specifico, la responsabilizzazione incide sulla legittimazione passiva, così come sull'onere probatorio.

Per quel che riguarda il primo aspetto, il GDPR si discosta dal regime precedente[196], stabilendo che a rispondere del danno sia tanto il titolare del trattamento, quanto il responsabile del trattamento, ossia entrambe le figure chiamate ad osservare il principio di *accountability*[197]. Per quanto attiene al secondo elemento, l'influenza della responsabilizzazione appare altrettanto evidente, giacché si assiste ad un'inversione dell'onere probatorio: il *controller* o il *processor* devono dimostrare la non imputabilità dell'evento dannoso, agevolando così la posizione del danneggiato, che può limitarsi a provare l'esistenza del trattamento,

[195] In questi termini, v. C. Bistolfi, L. Bolognini, E. Pelino, *op. ult. cit.,* p. 432.
[196]La Direttiva 95/46 CE, all' art. 23, par. 1, stabiliva che <<gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento [da intendere come titolare del trattamento]>>.
[197]La responsabilità del titolare e del responsabile è disciplinata all'art. 82, par. 1, GDPR.

il verificarsi del danno e la sussistenza di un nesso di causalità tra i due. In sostanza, per il principio di responsabilizzazione spetta a coloro che dispongono dei dati dimostrare la liceità del trattamento.

Da tali considerazioni, si evince che il principio di *accountability* delinea una responsabilità da trattamento illecito dei dati diversa rispetto a quella della Direttiva. Il nuovo modello si differenzia dal precedente per l'identificazione più immediata dei responsabili, nonché per la riduzione degli oneri a carico del danneggiato[198].

2.1. La responsabilità *ex* art. 23 della Direttiva 95/46 CE e la sua attuazione nella legislazione italiana

La responsabilità civile da trattamento illecito dei dati era stata disciplinata a livello europeo già prima dell'entrata in vigore del Regolamento, all'art. 23 della Direttiva 95/46 CE. Quest'ultimo, al primo paragrafo, imponeva agli Stati membri di garantire che chiunque fosse danneggiato da un trattamento illecito dei dati, ottenesse un risarcimento da parte del titolare[199]. Al paragrafo successivo, attribuiva al *controller* la facoltà di esonerarsi allorché fosse in grado di provare che l'evento dannoso non gli era in alcun modo imputabile. Grazie alla sua formulazione, la norma non pareva concedere molta discrezionalità ai legislatori nazionali, i quali, nel recepirla, dovevano necessariamente adottare una forma di responsabilità presunta a carico del solo titolare. Inoltre, la Direttiva, riconoscendo al *controller* la facoltà di discolparsi tramite la prova della non imputabilità del danno, sembrava ammettere una sola tipologia di responsabilità, quella oggettiva[200]. A riprova di quanto detto, vi era il considerando n. 55 della Direttiva, il quale disponeva che fosse esclusa la responsabilità del *controller* laddove questi dimostrasse <<l'esistenza di un errore della persona interessata o un caso di forza maggiore>>. Ebbene, il rimando ad una prova liberatoria che esulava completamente dalla colpa del responsabile, non faceva che collocare la responsabilità del titolare fra le

[198]Per approfondimenti sul rapporto tra il principio di *accountability* e la responsabilità civile, v. F. Albanese, I. Cardinali*, Il principio di responsabilizzazione (*accountability*),* cit., pp. 522 e ss.
[199]Malgrado il testo della Direttiva facesse riferimento al responsabile del trattamento, è stato ormai chiarito che ciò dipendeva da una traduzione impropria della locuzione, volendo l'interprete riferirsi al titolare del trattamento.
[200]Sui caratteri distintivi della responsabilità *ex* art. 23 della Direttiva 95/46 CE, v. G. Navone, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Le Nuove Leggi Civili Commentate*, 2022, n. 1, p. 132 e ss.

fattispecie di responsabilità oggettiva. Invero, a seconda del tipo di prova liberatoria contemplata dalla norma, è possibile valutare quale forma di responsabilità ricorre nella singola fattispecie: se la prova liberatoria riguarda la carenza di colpa, la fattispecie si pone in un sistema di responsabilità intermedio fra quella soggettiva e quella oggettiva; se la prova liberatoria viene fatta coincidere con il caso fortuito o la forza maggiore, intesi come eventi estranei del tutto inevitabili, le relative fattispecie si inseriscono nel sistema della responsabilità oggettiva[201].

In definitiva, nella Direttiva 95/46 CE, il legislatore europeo aveva optato per un modello di responsabilità presunta avente come prova liberatoria il caso fortuito, che avrebbe poi dovuto trovare attuazione nelle varie discipline nazionali[202].

In Italia, la Direttiva è stata attuata per la prima volta con la legge 31 dicembre 1996, n. 675[203], che dedicava due articoli al tema della responsabilità: l'art. 18 e l'art. 29, co. 9. Quanto all'art. 18, esso stabiliva che <<chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile>>. Malgrado l'espresso rimando all'art. 2050 c.c., il quale comportava un'inversione dell'onere della prova tale per cui colui che aveva provocato il danno, doveva dimostrare di aver adottato le misure idonee ad evitarlo, la formulazione della norma destava non poche perplessità. Tra le tante, essa non individuava il responsabile, ma rimetteva all'interprete il compito di risalirvi mediante la ricostruzione della sequenza causale che aveva prodotto il danno. Tale operazione risultava alquanto complessa se si considera un'altra caratteristica dell'art. 18, ossia che questo non esplicitava quali condotte erano da

[201]Così M. Comporti, *Le presunzioni di responsabilità*, in *Rivista di Diritto Civile*, 2000, n. 5, pp. 660 e ss.

[202]Una lettura parzialmente diversa è offerta da C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa e diritto privato*, 1998, n. 3, p. 672, il quale sostiene che il modello di responsabilità di cui all'art. 23 della Direttiva rappresenta <<un modello vuoto [...]. Nella specie il legislatore comunitario prevede che sia adottata una regola di responsabilità caratterizzata dalla possibilità di esonero per il soggetto individuato come destinatario della regola stessa. Lascia invece al legislatore nazionale la scelta del criterio d'imputazione. Questo, allora, può essere la colpa o un criterio oggettivo>>.

[203]La legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) è stata formalmente emanata in ottemperanza alla Convenzione 108. Da tale circostanza, e dall'assenza di riferimenti alla Direttiva 95/46 CE, come invece era richiesto dall'art. 32 della Direttiva, il quale prevedeva che le norme di attuazione richiamassero la legislazione europea, erano sorti dei dubbi sull'effettiva operatività delle tutele europee. Simili perplessità sono state successivamente superate, anche alla luce di quanto affermato da G. Tesauro, *Diritto Comunitario*, Cedam, Padova, 2001, p. 118, secondo il quale <<è ormai pacifico che l'attuazione di una direttiva non richiede necessariamente una riproduzione testuale delle sue disposizioni in una norma *ad hoc*>>.

ritenersi *non iure*, e quindi idonee a provocare un danno risarcibile. Oltretutto, l'art. 18 presentava lacune non trascurabili in materia di danno, poiché non precisava né le tipologie di danno risarcibili, né le modalità per quantificarlo[204].

In questo senso, un'unica indicazione proveniva dall'art. 29, co. 9, che faceva esplicitamente richiamo al danno non patrimoniale, puntualizzandone la risarcibilità <<anche nei casi di violazione dell'articolo 9>>[205]. Eppure, l'art. 29 non aveva sollevato meno dubbi dell'art. 18. *In primis,* rispetto alla collocazione del riferimento al danno non patrimoniale, dal momento che non si comprendeva cosa avesse spinto il legislatore a menzionarlo in quel punto, piuttosto che all'art. 18, rubricato <<danni cagionati per effetto del trattamento di dati personali>>[206]. In relazione al corpo del testo, invece, ci si domandava se tutte le violazioni dell'art. 9, l. n. 675/1996, determinassero un onere risarcitorio in capo al danneggiante, o solo alcune. Ancora, ci si interrogava sul tipo di regime probatorio utilizzabile per il danno non patrimoniale, ovvero se questo fosse da ricondursi, o meno, all'art. 2050 c.c. L'art. 29, infatti, non faceva alcun rimando in tal senso. Tuttavia, negare l'operatività del medesimo regime probatorio dell'art. 18, avrebbe comportato l'esistenza di due regimi contrapposti: uno, di cui al combinato disposto degli artt. 18 l. n. 675/1996 e 2050 c.c., applicabile in caso di danno patrimoniale; l'altro, di cui al combinato disposto degli artt. 29, co. 9, l. n. 675/1996 e 2059 c.c., applicabile in caso di danno non patrimoniale[207].

Nonostante le incertezze che avevano caratterizzato la regolazione della responsabilità nella legge 31 dicembre 1996, n. 675, il successivo Codice della privacy ha sostanzialmente confermato il regime precedente, facendo confluire la disciplina previgente nell'art. 15[208]. Tale articolo ha rappresentato, per il nostro

---

[204]Sulle criticità dell'art. 18 legge 31 dicembre 1996, n. 675, v. V. Colonna*, Il sistema della responsabilità civile da trattamento dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* vol. II, Milano, Giuffrè, 2003, p. 10 e ss.

[205]L'art. 9 legge 31 dicembre 1996, n. 675, rubricato <<modalità di raccolta e requisiti dei dati personali>>, stabiliva i criteri da osservare per il trattamento i dati personali, nonché quali di questi potessero costituirne l'oggetto.

[206]Circa la scelta legislativa di collocare il danno non patrimoniale all'art. 29, co. 9, l. 675/96, v. C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa e Diritto privato*, 1998, n. 3, pp. 682 e ss.

[207]Per ulteriori precisazioni sugli aspetti controversi dell'art. 29, co. 9, l. 675/96, v. F. Di Ciommo, *Vecchio e nuovo in materia di danno non patrimoniale da trattamento dei dati personali,* in *Danno e Responsabilità,* 2004, n. 10, pp. 817 e ss.

[208]Cfr. A. Riccobene, *Il danno cagionato per effetto del trattamento e i diversi modelli risarcitori*, in R. Panetta (a cura di), *Libera circolazione e protezione dei dati personali,* vol. II, Milano, Giuffrè, 2006, pp. 2021 e ss.

ordinamento, la tipizzazione dell'illecito civile conseguente al trattamento dei dati personali, nonché l'introduzione di una nuova fattispecie di responsabilità oggettiva. Del resto, se il legislatore avesse voluto attribuire alla responsabilità da trattamento illecito dei dati natura diversa da quella oggettiva, il suo intervento sarebbe apparso superfluo, potendo tale ipotesi ricadere automaticamente nell'alveo dell'art. 2043 c.c. Al contrario, l'art. 15 operava un espresso richiamo all'art. 2050 c.c., volendo in tal modo estendere al trattamento dei dati quanto stabilito dalla norma circa la prova liberatoria.

Meno plausibile appare l'interpretazione secondo cui il legislatore, rinviando all'art. 2050 c.c., intendesse includere il trattamento fra le attività pericolose. Difatti, anche considerando nel complesso le operazioni che rientrano nella nozione di trattamento, non emerge alcun pericolo intrinseco all'attività[209]. La pericolosità non poteva neppure essere desunta dalla tipologia di mezzi adoperati per il trattamento, poiché attribuire tale qualificazione sulla base degli strumenti impiegati, avrebbe comportato una limitazione arbitraria nell'applicazione del Codice della privacy, il quale operava indipendentemente dai mezzi adottati. Nello specifico, l'art. 15 si riferiva a qualunque danno derivante da una violazione del Codice, indipendentemente dalla pericolosità degli strumenti usati per il trattamento[210]. A sostegno di tali considerazioni, si poneva l'art. 37 del Codice; quest'ultimo, individuava le ipotesi di trattamento <<suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato>>, imponendo al titolare di comunicare al Garante per la protezione dei dati personali l'intenzione di avviare un trattamento di quel tipo. Dunque, il Codice riconosceva che alcuni trattamenti fossero potenzialmente idonei a provocare dei danni, ma neppure queste fattispecie venivano definite come pericolose. Alle medesime conclusioni, si perviene soffermandosi sulle attività regolate dal Testo Unico delle leggi in materia di pubblica sicurezza (TULPS)[211]. Il TULPS descrive come potenzialmente

[209]In questo senso, v. U. Ruffolo, *Dati personali: trattamento e responsabilità*, in V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1998, p. 284 e ss., il quale sostiene che, per quanto concerne il trattamento dei dati personali, <<siamo lontani da qualsiasi apprezzamento in termini di pericolosità>> sia sotto l'aspetto quantitativo, ossia della potenzialità dannosa del trattamento, sia sotto quello qualitativo, relativo all'entità del danno.

[210]Così A. Riccobene, *Il danno cagionato per effetto del trattamento e i diversi modelli risarcitori*, cit., pp. 2059 e ss.

[211]Il Testo Unico delle leggi di pubblica sicurezza (TULPS), approvato con il Regio Decreto 18 giugno 1931, n. 773, è una raccolta delle varie disposizioni legislative inerenti la sicurezza pubblica.

pericolose, e perciò tali da giustificare l'intervento della forza pubblica, attività come: l'utilizzo di armi, la realizzazione di esplosioni, l'impiego di gas tossici e molte altre ancora. Ebbene, nessuna di queste condotte sembra minimamente paragonabile a quelle che rientrano nel trattamento dei dati[212].

In conclusione, il trattamento dei dati personali costituisce un'attività "neutra", che, tuttavia, può provocare un danno all'interessato allorché il soggetto agente ponga in essere una condotta pericolosa[213].

Dall'impossibilità di sussumere il trattamento dei dati sotto la categoria delle attività pericolose, consegue che il rinvio all'art. 2050 c.c. servisse solo ad estendere a tale ambito l'inversione dell'onere probatorio: colui che provoca il danno deve dimostrare di aver adottato tutte le misure idonee ad evitarlo[214]. La prova liberatoria, quindi, non riguardava le modalità della condotta, ovvero se il danneggiante avesse agito con dolo o colpa, bensì le modalità organizzative dell'attività pericolosa, vale a dire se il danneggiante avesse adottato misure adeguate a prevenire l'evento dannoso. È ormai pacifico che queste misure non coincidevano né con le misure minime di sicurezza, di cui all'Allegato B del Codice[215], le quali, se adottate, escludevano la responsabilità penale del titolare[216], né tanto meno con le misure preventive di cui all'art. 31 del Codice[217]. Tali misure

---

[212] Cfr. A. Riccobene, *op. ult. cit*., pp. 2060 e ss.

[213]Nella giurisprudenza italiana, v. Cass. 23 febbraio 1983, n. 1394, in *Mass. Giur. it.*, 1983, la quale precisa che le attività pericolose sono. quelle pericolose in sé, per la natura o i mezzi adoperati; oppure, quelle che le norme definiscono tali. Di certo, non rientrano fra le attività pericolose le ipotesi in cui la pericolosità scaturisce dagli errori o dalle colpe dell'agente nell'uso degli strumenti adottati.

[214]Su posizioni simili, seppur con riferimento all'art. 18 della L. 675/96, v. M. Berlingieri, *La responsabilità civile derivante dal trattamento dei dati personali: natura giuridica, conseguenze, oneri probatori*, 2001, disponibile *online* su https://www.privacy.it/archivio/berlingieri04.html.

[215]L'Allegato B del Codice della privacy (Disciplinare tecnico in materia di misure minime di sicurezza**),** abrogato dall'art. 27, co. 1, lett. d), del d.lgs. 10 agosto 2018, n. 10, distingueva fra misure minime per trattamenti con strumenti elettronici, in cui rientravano, ad esempio, l'autenticazione informatica e le procedure di gestione delle credenziali di autorizzazione, e misure minime per trattamenti senza strumenti elettronici, come le procedure per la custodia degli atti affidati al responsabile del trattamento.

[216]Ai sensi dell'art. 169 Codice della privacy, abrogato dal d.lgs. n. 101/2018, colui che ometteva di adottare le misure minime era punibile con l'arresto fino a due anni.

[217]Le misure *ex* art. 31 del Codice della privacy, anch'esso abrogato dal d.lgs. n. 101/2018, miravano a prevenire <<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 della raccolta>>.

erano volte a ridurre al minimo i pericoli connessi alla gestione dei dati, ma non per questo erano sufficienti ad impedire il danno[218].

Parte della dottrina ha altresì escluso che la prova liberatoria di cui all'art. 2050 c.c. potesse essere identificata con il caso fortuito, in quanto dimostrare di aver attuato misure idonee ad evitare il danno è diverso dal provare il fortuito. Nel primo caso, la responsabilità del danneggiante non si configura; nel secondo, si verifica un'interruzione del nesso causale tale da escludere la responsabilità di chi agisce[219].

Al suddetto orientamento se ne contrapponeva uno diametralmente opposto, secondo cui la prova liberatoria dell'art. 2050 c.c. agiva sul rapporto di causalità, giacché la dimostrazione delle misure idonee ad evitare il danno esonerava il danneggiante solo quando egli fosse riuscito a provare l'interruzione del nesso causale; pertanto, a parere di questa dottrina, la prova liberatoria in esame era da intendersi come la << dimostrazione indiretta del caso fortuito, nel senso che esclude sul piano causale la rilevanza dell'attività pericolosa rispetto all'evento dannoso>>[220].

Benché vi fossero visioni contrastanti sulla natura delle misure idonee, la dottrina non nutriva alcun dubbio che queste non fossero determinabili *a priori* dal titolare del trattamento, il quale doveva individuare le più adeguate al caso di specie. Oltre a questo, vi era un altro aspetto dell'art. 15 del Codice che appariva pacifico: esso ammetteva la risarcibilità tanto del danno patrimoniale, quanto del danno non patrimoniale da trattamento illecito dei dati. A riprova di ciò, vi era il secondo comma dell'articolo in esame, introdotto dal legislatore proprio per ampliare il novero dei <<casi determinati dalla legge>> di cui all'art. 2059 c.c. e fugare ogni dubbio circa la risarcibilità del danno non patrimoniale[221].

---

[218]Sulla distinzione tra le misure preventive e la prova liberatoria di cui all'art. 15 Codice della privacy, v. A. Riccobene, *Il danno cagionato per effetto del trattamento e i diversi modelli risarcitori*, cit., pp. 2059 e ss.

[219]Per tutti, v. C. Salvi, *Responsabilità extracontrattuale (dir. vig.),* in *Enciclopedia del diritto*, vol. XXXIX, Milano, Giuffrè, 1988, pp. 1234 e ss.

[220]M. Franzoni, *Responsabilità derivante da trattamento dei dati personali*, in G. Finocchiaro, F. Delfini (a cura di), *Diritto dell'informatica,* Torino, UTET, 2014, p. 833.

[221]Per un'analisi approfondita sulla risarcibilità dei danni non patrimoniali nel Codice della privacy, v. F. Di Ciommo, *Il danno non patrimoniale da trattamento dei dati personali*, in G. Ponzanelli (a cura di), *Il "nuovo" danno non patrimoniale*, Padova, Cedam, 2004, pp. 255 e ss.

2.1.1. Cenni sull'attuazione della responsabilità *ex* art. 23 della Direttiva 95/46 CE nelle legislazioni europee

Per quanto riguarda gli altri Stati membri, ognuno di essi aveva recepito il sistema di responsabilità della Direttiva all'interno del proprio ordinamento. Tuttavia, ciascuno dei Paesi dell'Unione presentava un panorama giuridico ben distinto, ragion per cui si riscontravano delle differenze sia rispetto alla tipologia di danno risarcibile, sia rispetto alla possibilità di esonerare il *controller*.

Secondo le leggi del Belgio e del Portogallo, ad esempio, il titolare del trattamento era tenuto a risarcire il danno, a meno che non dimostrasse di non essere responsabile per l'evento che aveva arrecato nocumento. La legge danese esprimeva il principio in termini ancora più dettagliati, affermando che il *controller* fosse responsabile per qualsiasi danno derivante da un trattamento dei dati violativo della legge sulla *data protection*. Al fine di discolparsi, il titolare avrebbe dovuto provare l'inevitabilità dell'evento dannoso, ossia che questo si sarebbe verificato anche laddove fosse stata impiegata la diligenza e la cura richiesta dal trattamento. Nei Paesi Bassi, la legge prevedeva che l'ammontare del danno risarcibile fosse ridotto a seconda del grado di responsabilità accertato in giudizio, applicando le norme ordinarie in materia di responsabilità. Allo stesso modo, in Finlandia, Francia e Lussemburgo trovavano attuazione le norme ordinarie sulla responsabilità civile e amministrativa. In Irlanda, la normativa considerava un illecito qualunque violazione della legge sulla protezione dei dati, stabilendo che i titolari avevano un onere di diligenza nei confronti degli interessati. Una situazione analoga si aveva anche nel Regno Unito, ove la legge ammetteva il risarcimento per i danni conseguenti alle inosservanze del *data controller*, a prescindere da quanto queste fossero gravi. Pur riconoscendo il diritto risarcitorio nella quasi totalità dei casi, la disciplina anglosassone poneva dei limiti rispetto al tipo di danno risarcibile: perché il *data subject* fosse ristorato del danno non patrimoniale subito, doveva essere altresì raggiunta la prova del danno patrimoniale.

In definitiva, i legislatori europei avevano ottemperato alla Direttiva traslando la responsabilità da trattamento illecito dei dati nei propri ordinamenti, senza però uniformarsi. Difatti, vi erano divergenze significative su quali condotte configurassero l'illecito, nonché sulla risarcibilità del danno non patrimoniale. Nella pratica, questo comportava che il titolare fosse sottoposto a trattamenti diversi

a seconda di come veniva regolata la sua responsabilità, la quale, come evidenziato, non sempre era destinataria di una disciplina *ad hoc*[222].

3. La responsabilità *ex* art. 82 GDPR: gli elementi costitutivi della fattispecie

In un contesto connotato, da una parte, dalla frammentazione legislativa, dall'altra, da un processo di innovazione tecnologica che poneva nuove sfide in materia di responsabilità, si inseriva l'aspirazione dell'Unione ad uno *european tort law*. D'altronde, era ormai evidente che fosse necessario adottare un sistema di regole uniformi in materia di responsabilità civile[223]. In quest'ottica, il legislatore europeo ha inserito l'art. 82 all'interno del Regolamento.

Per cogliere a pieno la portata innovatrice della norma, occorre dapprima analizzarne gli elementi strutturali.

I danneggiati

Il primo elemento da considerare è quello dei danneggiati, ovvero i soggetti che l'art. 82 GDPR legittima ad agire verso i responsabili. Questo aspetto viene disciplinato al primo paragrafo dell'articolo, laddove si stabilisce che <<chiunque subisca un danno>> ha diritto ad essere risarcito. A tal riguardo, si sono sviluppati due orientamenti differenti: uno ha attribuito al termine <<chiunque>> un significato estensivo, riconoscendo la facoltà risarcitoria a tutti coloro che subiscano un danno causalmente collegato ad un trattamento illecito dei dati, indipendentemente dalla loro qualificazione come interessati[224]. L'altro, dando rilievo alla circostanza che anche la Direttiva si riferiva ai danneggiati come a <<chiunque>>[225], ha interpretato l'espressione in senso restrittivo. In particolare,

[222]Sulla regolazione della responsabilità del titolare nella legislazione europea, v. *Report on the findings of the study*, in *EC Study on implementation of data protection directive*, cit., pp. 168 e ss.
[223]Una tendenza opposta ha invece caratterizzato gli Stati Uniti, i quali hanno preferito disciplinare la tutela dei dati con normative statali, piuttosto che a livello federale. Secondo C. Masieri, *La tutela dei dati personali relativi alla salute: approccio europeo ed americano a confronto*, in R.E. Cerchia (a cura di), *Percorsi di diritto comparato*, Milano, Milano University Press, 2021, pp. 199 e ss., l'assenza di una regolazione unitaria non sarebbe riconducibile a delle <<limitazioni formali di competenza in capo agli organi legislativi federali>> ma sarebbe una vera e propria scelta di *policy.*
[224]A favore di una lettura allargata del termine <<chiunque>>, v. M. Ratti*, La responsabilità da illecito trattamento dei dati personali nel nuovo Regolamento*, in Finocchiaro G. (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* cit., pp. 615 e ss.
[225]Ai sensi dell'art. 23, par. 1, della Direttiva 95/46 CE (v. nota 52).

questa dottrina ha sostenuto che, se la responsabilità dell'art. 82 GDPR ha lo stesso fondamento di quella della Direttiva, cioè il rapporto obbligatorio instauratosi tra *controller*, *processor* e *data subject*, non può esservi differenza neppure rispetto alla figura del danneggiato. Di conseguenza, nel GDPR, come nella Direttiva, solo l'interessato può richiedere un indennizzo per il pregiudizio subito[226]. Malgrado ciò, l'orientamento in esame non ha escluso che soggetti diversi dall'interessato possano avanzare una pretesa risarcitoria, laddove subiscano un pregiudizio a causa di una gestione scorretta dei loro dati. Semplicemente, in quel caso la responsabilità degli attori del trattamento non avrebbe titolo nell'art. 82 GDPR, bensì nell'art. 2043 c.c., per quanto riguarda la disciplina italiana, e nelle disposizioni corrispondenti per quanto concerne gli altri Stati membri.

È indubbio che l'art. 82 GDPR rimandi all'art. 23 della Direttiva. Eppure, tale affermazione non può costituire la conclusione del ragionamento, dal momento che il Regolamento ha introdotto una novità significativa rispetto alla Direttiva, ossia che i dati di cui dispongono il titolare e il responsabile possono altresì appartenere ad un minore di sedici anni, purché egli abbia acconsentito al trattamento (art. 8 GDPR)[227]. Ebbene, l'art. 82, par. 1, GDPR non fa alcun riferimento né all'ipotesi che il minorenne possa subire un pregiudizio dal trattamento, né tantomeno che questi, al pari dell'interessato maggiorenne, sia legittimato ad agire per il risarcimento. A fronte di un simile vuoto normativo, la dottrina ha finito per estendere alla fattispecie il principio per cui il titolare di un diritto ha anche il potere di agire in sua difesa. D'altra parte, non si comprende come un minore possa essere capace di esercitare un diritto, e non di tutelarlo in via giudiziaria[228]. Così come per il minorenne, il fatto che il GDPR non annoveri espressamente soggettivi diversi dal *data subject* fra i danneggiati, non significa

[226]Tra tutti, v. F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 456 e ss.

[227]Per approfondimenti sul consenso del minore al trattamento dei dati, v. F. Naddeo, *Il consenso al trattamento dei dati personali del minore*, in *Diritto dell'informazione e dell'informatica,* 2018, n. 1, pp. 27 e ss.

[228]Sugli ostacoli che il minore incontra ogniqualvolta voglia far valere personalmente i propri diritti in sede giudiziale, v. F. Tommaseo*, Rappresentanza e difesa del minore nel processo civile*, in *Famiglia e Diritto,* 2007, n. 4 p. 411 e ss., secondo il quale il minorenne spesso <<non ha modo di far sentire la propria voce in condizioni di oggettiva ed effettiva parità con le parti "adulte>> anche quando i procedimenti riguardano i suoi diritti fondamentali.

che questi non possano essere lesi da un trattamento illecito dei dati e, quindi, avanzare una pretesa risarcitoria[229].

I danneggianti

Identificati i danneggiati, è necessario chiarire quali siano i soggetti tenuti a risarcirli per il pregiudizio patito. Tale informazione si ricava, ancora una volta, dal primo paragrafo dell'art. 82 GDPR, ove si afferma che il *controller* e il *processor* devono rispondere del danno derivante dall'inosservanza del Regolamento. L'affermazione non stupisce, se si considera che nel GDPR il legislatore europeo ha aderito a una logica preventiva, in virtù della quale ha rivisto la funzione della responsabilità da trattamento illecito dei dati. Quest'ultima ha conservato la funzionalità tipica della responsabilità civile, vale a dire quella reintegrativo compensativa[230], ma ne ha acquisiste anche delle nuove.

Quanto alla funzione primaria della responsabilità, è innegabile che sia ancora quella di garantire al danneggiato l'integrale riparazione dal danno. In questo senso, può essere letto il diritto del danneggiato di essere risarcito per qualunque pregiudizio, materiale o immateriale che sia[231]; nonché l'onere dello stesso di provare il *quantum* esatto del danno, al fine di ottenere il pieno ristoro della perdita subita[232]. Benché la responsabilità di cui all'art. 82 GDPR sia ancora animata da una volontà reintegrativo – compensativa, il legislatore europeo ne accentua la funzione sanzionatoria. Tuttavia, è bene precisare che tale funzionalità

---

[229]In senso critico, v. F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 456.

[230]La letteratura sulla funzione reintegrativo-compensativa della responsabilità da trattamento illecito dei dati personali è sconfinata: *ex multis,* P. Ziviz, *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla Legge 675/1996*, in *Responsabilità civile e previdenza*, 1997, pp. 1307 e ss.; G. Resta , A. Salerno, *La responsabilità civile per il trattamento dei dati personali*, in G. Alpa, G. Conte (a cura di), *La responsabilità d'impresa*, Milano, Giuffrè, 2015, pp. 658 e ss; A. Di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. Cuffaro, V. Ricciuto, V. Zeno Zencovich (a cura di), *Trattamento dei dati e tutela della persona,* cit., p. 238 ss.

[231]La risarcibilità del danno materiale e immateriale è sancita al primo paragrafo dell'art. 82 GDPR.

[232]Ai fini risarcitori, il danneggiato deve dimostrare l'esistenza del danno, la sua entità, la violazione della normativa sulla protezione dei dati personali e il nesso causale tra questi elementi. Dal canto suo, il titolare, o il responsabile, che voglia sottrarsi all'onere risarcitorio, deve provare che il danno non gli è in alcun modo attribuibile. Così, R. Goretta, *Risarcimento danni per violazione del GDPR, ecco chi paga e quanto***,** settembre 2019, disponibile *online* su https://www.agendadigitale.eu/sicurezza/privacy/risarcimento-danni-per-violazione-del-gdpr-ecco-chi-paga-e-quanto/.

non ha una finalità punitiva[233], quanto piuttosto quella di assicurare l'efficacia deterrente della norma rispetto ai titolari e ai responsabili del trattamento. A conferma di ciò, si pone l'aumento degli obblighi per il *controller*, come pure l'introduzione di oneri in capo al *processor*, in ottemperanza al principio di *accountability* che permea l'intero Regolamento. Ad una logica di deterrenza, sembra rispondere anche la previsione sull'onere probatorio del titolare e del responsabile, che risulta essere particolarmente gravoso per entrambi (art. 82, par. 3, GDPR)[234]. Oltre a trovare riscontro nel testo del Regolamento, la funzione preventivo-deterrente della responsabilità ha un intento evidente alla base: adeguare il sistema della responsabilità al *risked based approach* che caratterizza la normativa sulla *data protection.*

In definitiva, il regime di responsabilità dell'art. 82 GDPR non mira solo a risarcire i danni, bensì a prevenirli e sanzionare i responsabili. In questa prospettiva, impone a *controller* e *processor* di agire con maggior cautela[235].

Tra l'altro, siffatta interpretazione dell'art. 82 GDPR risulta coerente con due ulteriori disposizioni del Regolamento: l'art. 26, il quale autorizza l'interessato a far valere, nei confronti dei contitolari, gli stessi diritti che egli vanta nei confronti del titolare; l'art. 27, il quale, nell'eventualità in cui sia designato un rappresentante del trattamento, ammette che il *data subject* eserciti contro di lui le medesime azioni che eserciterebbe avverso *controller* e *processor*, inclusa quella risarcitoria[236].

Il danno risarcibile

In ultimo, occorre soffermarsi sull'elemento del danno per comprendere quale possa ritenersi risarcibile alla luce del Regolamento. Tale informazione si ricava da un'analisi congiunta dell'art. 82, par. 1, GDPR, che ammette il risarcimento di danni materiali e immateriali, e del considerando 146. Quest'ultimo

---

[233]In questa prospettiva si muovono le conclusioni dell'avvocato generale M. Campos Sànchez-Bordona, presentate il 6 ottobre 2022, nella causa C-300/21, *UI v. Österreichische Post AG*, par. IV, il quale ha affermato che <<dal punto di vista letterale […] l'RGPD non consente di prevedere un risarcimento di carattere punitivo>>.

[234]Ai sensi dell'art. 82, par. 3, del GDPR << Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità […] se dimostra che l'evento dannoso non gli è in alcun modo imputabile>>.

[235]Cfr. M. Gambino, *Principio di responsabilità e tutela aquiliana dei dati personali*, in P. Perlingieri (diretto da), *Quaderni della Rassegna di diritto civile,* Napoli, Edizioni Scientifiche Italiane, 2018, pp. 135 e ss.

[236]Sulla figura del rappresentante del trattamento, come pure sul ruolo che questi e il contitolare assumono nel sistema di responsabilità dell'art. 82 GDPR, si dirà meglio più avanti.

mira ad assicurare al *data subject* un'effettiva compensazione per la lesione patita; pertanto, esorta la giurisprudenza europea a fornire un'interpretazione ampia del termine danno[237]. Le corti nazionali, dal canto loro, sono state storicamente caute nel concedere risarcimenti per pregiudizi non materiali, spesso richiedendo la prova di un danno specifico. In una recente caso olandese, ad esempio, la Corte Suprema dei Paesi Bassi ha stabilito che, quando si richiedono danni immateriali, il ricorrente deve avvalorare la propria pretesa con dati concreti[238]. Un simile approccio sembra essere in linea con la consolidata giurisprudenza locale in tema di danni morali, secondo cui l'accertamento di detti danni deve avvenire sulla base di criteri oggettivi[239].

Dalla casistica esaminata emerge che, nell'ambito del GDPR, le sfide relative ai danni immateriali sono principalmente due: dimostrarli e valutarli. Invero, pregiudizi come il disagio emotivo, la perdita di reputazione e la violazione della privacy ledono la sfera personale dell'individuo, aspetto che rende difficile verificarli. A riprova di questa difficoltà, vi sono anche le pronunce della Corte di Giustizia, che, in alcuni casi, ha condizionato la risarcibilità del danno immateriale alla dimostrazione del nesso causale tra la condotta lesiva e il danno subito[240]; in altri, ha richiesto la prova di una lesione reale e certa[241]. Le diverse posizioni assunte dalla Corte sono riconducibili alla particolare natura del danno immateriale, la quale lascia ai giudici ampio margine di discrezionalità nel riconoscerne, o meno, l'esistenza.

La dimostrazione non è l'unica criticità dei pregiudizi immateriali, dal momento che l'art. 82 GDPR non offre un metodo standardizzato per quantificarli, demandando il compito alle corti europee. Questo approccio comporta che gli Stati membri applicano criteri diversi per determinare l'ammontare del risarcimento, con

[237]Il considerando 146 si riferisce impropriamente alla Corte di Giustizia, volendo in realtà intendere le Corti dei singoli Stati membri. In questi termini, v. V. A. Ghaziani, M. A. Ghaziani, M. A. Ghaziani, *Assessing Non-Material Damages Under the GDPR: A Review of The Recent Judicial Practice of Germany, UK, and the Netherlands*, in *Revista Jurídica Portucalense,* 2022, n. 32, pp. 280 e ss.

[238]Supreme Court of the Netherlands, 15 marzo 2019, n. 17/04668, disponibile *online* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2019:376.

[239]Supreme Court of the Netherlands, 9 maggio 2003, n. C01/246HR, disponibile *online* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2003:AF4606

[240]Corte di Giustizia dell'Unione Europea, 14 maggio 1998, C-259/96, *Council of the European Union v. Lieva de Nil and Christiane Impens*, disponibile *online* su www.curia.europa.it.

[241]Corte di Giustizia dell'Unione Europea, 4 aprile 2017, C-337/15 P, *European Ombudsman v. Claire Staelen*, disponibile *online* su www.curia.europa.it.

esiti di incoerenza e discrezionalità giudiziaria. A titolo esemplificativo, le corti anglosassoni liquidano i danni immateriali secondo le "*Guidelines for the Assessment of General Damages in Personal Injury Cases" del Judicial College"*, le quali individuano dei valori di riferimento sulla scia di precedenti giurisprudenziali[242]. In Francia, invece, i giudici nazionali si servono di tabelle di riferimento, conosciute come "*Référentiel Mornet*"[243]. Inoltre, come si approfondirà meglio in seguito, alcune corti europee adottano il criterio secondo cui la lesione deve raggiungere una soglia minima di gravità per essere risarcita (ad es. Germania), mentre altre se ne discostano (ad es. Francia e Belgio)[244].

Dunque, se è vero che il GDPR mira a garantire agli interessati il pieno ristoro del pregiudizio patito, è altresì vero che la normativa lascia irrisolte diverse questioni sulla dimostrazione e sulla valutazione dei danni immateriali. Benché il considerando 146 auspichi che siano i giudici nazionali, tramite un'interpretazione ampia del concetto di danno, a colmare tali lacune, ciò non appare possibile finché il legislatore non fornisca loro dei criteri per provare l'esistenza dei danni immateriali e misurarne l'entità[245].

Il danno risarcibile nell'ordinamento giuridico italiano

Dalle osservazioni svolte, si evince che il danno immateriale può essere risarcito all'interno dell'ordinamento europeo; infatti, il legislatore comunitario ammette la risarcibilità tanto del danno materiale, quanto di quello immateriale. Eppure, questo binomio non sembra corrispondere perfettamente a quello adoperato nell'ordinamento italiano, che distingue tra danno patrimoniale e non patrimoniale.

La diversa formulazione adottata aveva suscitato delle riserve riguardo la risarcibilità del danno non patrimoniale derivante da trattamento illecito dei dati. In particolare, deponeva in senso negativo l'abrogazione dell'art. 15 del Codice della privacy, poiché veniva meno l'esplicito riferimento al danno non patrimoniale ivi

---

[242]Cfr. Judicial College, *Guidelines for the Assessment of General Damages in Personal Injury Cases*, Oxford, Oxford University Press, 2024.

[243]Sulla quantificazione del danno immateriale in Francia, v. B. Mornet, *L'indemnisation des Prejudices en cas de blessures ou de décès,* settembre 2021, disponibile *online* su https://www.fac-droit.univ-smb.fr/wp-content/uploads/2022/10/Referentiel-dit-Mornet-septembre-2022.pdf.

[244]Per un'analisi approfondita dei criteri di risarcibilità del danno immateriale nel panorama giuridico europeo, v. J. Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, in *European Journal of Privacy Law & Technologies*, vol. XIII, 2022, n. 2, pp. 147 e ss.

[245]Così V. A. Ghaziani, M. A. Ghaziani, M. A. Ghaziani, *Assessing Non-Material Damages Under the GDPR: A Review of The Recent Judicial Practice of Germany, UK, and the Netherlands,* cit., pp. 284 e ss.

contenuto. Altri argomenti, però, facevano propendere per l'estensione della pretesa risarcitoria al danno non patrimoniale, fra i quali quello della costanza terminologica. Questo evidenzia come l'espressione "danno non patrimoniale" o "danno morale" sia ampiamente utilizzata nei sistemi giuridici di influenza francese quali l'Italia, la Spagna (*daño moral*) e il Belgio (*dommage moral*); mentre, in altri ordinamenti ci si riferisca a tale categoria con la locuzione di "danno immateriale". È questo il caso della Germania, in cui si parla di "*nicht Vermögensschaden*", ovvero pregiudizio immateriale. L'adozione, da parte di alcuni ordinamenti, della terminologia del GDPR per indicare il danno non patrimoniale contribuisce così a superare le riserve della dottrina e giurisprudenza italiana circa la sua risarcibilità[246].

Il suesposto argomento non è l'unico a confutare la tesi secondo cui il risarcimento del danno non patrimoniale sarebbe inesigibile. In questo senso depone altresì il considerando n. 85, il quale elenca, in maniera esemplificativa, i danni che potrebbero derivare dalla violazione dei dati personali, includendovi <<pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale>>. Questi esempi rientrano nella definizione di danno non patrimoniale formulata dalla giurisprudenza nazionale, che fa coincidere tale categoria di danno con quello derivante dalla lesione di interessi legati alla persona, privi di rilevanza economica[247]. Ancora una volta, si può affermare che il danno non patrimoniale corrisponde a quello immateriale. D'altronde, elementi a sostegno di questa conclusione si riscontrano sia nell'ipotesi in cui si identifichi la responsabilità *ex* art. 82 GDPR con una forma di responsabilità extracontrattuale, e quindi si applichi l'art. 2059 c.c.; sia che si qualifichi la responsabilità del Regolamento come una responsabilità contrattuale. Nel primo caso, l'argomento principale è che il Regolamento europeo, nella gerarchia delle fonti, è equiparabile alla legge; pertanto, sarebbe soddisfatto il requisito dell'espressa previsione legislativa di cui all'art. 2059 c.c. Qualora si prediliga la tesi della responsabilità contrattuale, invece, il problema della risarcibilità del danno non patrimoniale non si pone, giacché nel codice civile non esiste alcuna disposizione che, in caso di

[246]Per una comparazione delle caratteristiche del danno non patrimoniale nei sistemi giuridici europei, v. V. V. Palmer, *The Recovery of non- pecunary loss in European Contract Law,* in V.V. Palmer (a cura di), *The Common Core of European Private Law*, Cambridge, Cambridge University Press, vol. IV, 2015, pp. 4 e ss.
[247]Cass. 11 novembre 2008, n. 26972, in *Rep. Foro It*., 2008, voce *Danni in materia civile*, n. 309.

inadempimento, circoscriva il risarcimento al solo danno patrimoniale. Piuttosto, l'art. 1218 c.c. disciplina la responsabilità contrattuale senza specificare alcunché sul tipo di danno risarcibile, così da ricomprendervi ogni tipologia[248].

Le considerazioni svolte suggeriscono che il legislatore europeo avrebbe potuto compiere una scelta giuridicamente più corretta, impiegando il binomio danno patrimoniale e non patrimoniale al posto di quello adottato; malgrado ciò, si è giunti alla conclusione che i sintagmi "danno materiale" e "danno immateriale" coincidano con le locuzioni dell'abrogato art. 15 Codice della privacy, ovvero danno patrimoniale e non patrimoniale.

In ordine a tale ultima categoria di danno, parte della dottrina ha sostenuto che l'esplicito riferimento alla sua risarcibilità, prima nel Codice della privacy, poi all'art. 82 GDPR, dovrebbe essere letto come una valutazione *ex ante* di offensività. Difatti, il legislatore, consapevole che un illecito trattamento dei dati provoca raramente pregiudizi di natura patrimoniale, e più di frequente pregiudizi non patrimoniali, giacché lede i diritti fondamentali di riservatezza e protezione dei dati personali, avrebbe risolto a monte la questione dell'*an debeatur*, lasciando insoluta solo la determinazione del *quantum.* Se così fosse, il caso di specie configurerebbe un'ipotesi di danno *in re ipsa*, poiché l'inosservanza delle norme di condotta che regolano il trattamento costituirebbe, di per sé, un danno[249].

D'altra parte, la giurisprudenza di legittimità ha fermamente escluso che l'art. 82 del GDPR abbia introdotto un danno *in re ipsa*, interpretandolo piuttosto come un "danno-conseguenza" ai sensi dell'art. 2043 c.c. In questo senso, la Suprema Corte[250] ha ribadito che, quand'anche fosse leso un diritto fondamentale come quello alla *data protection*, dovrebbe ugualmente essere esperito un giudizio sulla "gravità della lesione" e sulla "serietà del danno", per verificare l'effettivo pregiudizio alla sfera personale del danneggiato[251]. Un simile orientamento si

[248]In questi termini, v. F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 465 e ss.

[249]Per tutti, v. E. Tosi, *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: Funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo,* in *Contratto e Impresa*, 2020, n. 3, pp. 1134 e ss.

[250]Tra le principali pronunce della Suprema Corte, si possono segnalare: Cass. 8 gennaio 2019, n. 207, in *Massimario.it*, 2019, VI, con nota di M. E. Bagnato, *Illecita segnalazione alla Crif? Il danno deve essere provato dall'interessato;* Cass. 5 marzo 2015, n. 4443, in *Rep. Foro it*., 2015, voce *Spese giudiziali in materia civile,* n. 78; Cass. 5 settembre 2014, n. 18812, *in Foro it.*, 2015, I, 119.

[251]La Corte di Cassazione ha precisato che <<la gravita della lesione attiene al momento determinativo dell'evento dannoso, quale incidenza pregiudizievole sul diritto o interesse

conforma a quanto già sostenuto dalla Sezioni Unite in materia di danno non patrimoniale, le quali hanno stabilito l'imprescindibilità del "doppio filtro" nell'accoglimento di una pretesa risarcitoria[252]. In virtù di tale filtro, l'offesa ad un diritto inviolabile non è di per sé sufficiente a giustificare un risarcimento, ma occorre che la lesione ecceda una determinata soglia di tollerabilità, determinando un danno serio. Diversamente, non si opererebbe un corretto bilanciamento tra il principio di solidarietà[253] nei confronti del danneggiato e quello di tolleranza[254], che finirebbe per soccombere ogniqualvolta fosse violato un diritto fondamentale.

In proposito, i sostenitori del danno *in re ipsa* replicano che l'attuazione del doppio filtro provocherebbe un'asimmetria regolatoria, in quanto il meccanismo verrebbe applicato al pregiudizio non patrimoniale e non a quello patrimoniale. Inoltre, si assisterebbe ad una riduzione di tutela dei diritti costituzionalmente garantiti, poiché, ai fini risarcitori, la loro violazione dovrebbe comunque superare il vaglio della gravità e serietà della lesione[255].

Da tali ragionamenti deriva la crescente propensione all' "oggettivazione" del danno da trattamento illecito dei dati; tuttavia, è opportuno segnalare che, a

---

selezionato (dal legislatore o dall'interprete) come meritevole di tutela aquiliana, e la sua portata è destinata a riflettersi sull'ingiustizia del danno che non potrà più predicarsi tale in presenza di una minima offensività della lesione stessa>>. Mentre, la serietà del danno concerne <<il piano delle conseguenze della lesione e cioè l'area dell'obbligazione risarcitoria, che si appunta sulla effettività della perdita subita (il c.d. danno-conseguenza); il pregiudizio "non serio" esclude che vi sia una perdita di utilità derivante da una lesione che pur abbia superato la soglia di offensività>>: così Cass. 19 settembre 2014, n. 19834, *in Rep. Foro it.,* 2014*,* voce *Locazione,* n. 75.

[252]Cass. sez. un. 11 novembre 2008, nn. 26972, 26973, 26975 (note come Sentenze Gemelle di San Martino). Tra i diversi commenti apparsi sulle principali riviste giuridiche: in *Dir. fam. pers*., 2009, I, 73 con nota di F. Gazzoni, *Il danno esistenziale, cacciato, come meritava, dalla porta, rientrerà dalla finestra*; in *Giur. it.,* 2009, 259, con nota di G. Cassano, *Danno non patrimoniale ed esistenziale: primissime note critiche a Cassazione civile, Sezioni Unite, 11 novembre 2008, n. 26972*; in *Giur. it.,* 2009, 317, con nota di V. Tomarchio, *L'unitarietà del danno non patrimoniale nella prospettiva delle Sezioni unite*; in *Riv. dir. civ*., 2009, II, 97, con nota di F. D. Busnelli*, Le sezioni unite e il danno non patrimoniale*; in *Resp. civ. e prev*., 2009, 38, con note di P.G. *Monateri, Il pregiudizio esistenziale come voce del danno non patrimoniale*; E. Navarretta, *Il valore della persona nei diritti inviolabili e la complessità dei danni non patrimoniali*; D. Poletti, *La dualità del sistema risarcitorio e l'unicità della categoria dei danni non patrimoniali.* Mediante le pronunce in esame, la Suprema Corte ha chiarito quali sono i criteri per il risarcimento del danno non patrimoniale di cui all'art. 2059 c.c, ribadendo che tale danno è risarcibile soltanto nei casi in cui sia espressamente previsto dalla legge, come quando un illecito civile integri un reato; oppure, quando il risarcimento sia giustificato da un'interpretazione costituzionalmente orientata dell'art. 2059 c.c., vale a dire allorché sia leso gravemente un diritto fondamentale.

[253]Per un'analisi puntuale del principio di solidarietà in ambito di *data protection*, v. F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di cassazione*, in *Contratto e Impresa*, 2023, n. 2, pp. 405 e ss.

[254] Sul principio di tolleranza, v. A. Musio, *Il principio di tolleranza nel diritto civile*, in *Contratto e Impresa*, 2017, n. 2, pp. 403 e ss.

[255]Cfr. E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale,* Milano, Giuffrè, 2020, pp. 253 e ss.

livello giurisprudenziale, permane la tendenza ad ammettere il risarcimento del danno non patrimoniale solo laddove sia provato il danno conseguenza.

3.1. La responsabilità per illecito trattamento dei dati. Una natura giuridica controversa

L'introduzione del Regolamento ha obbligato gli Stati membri a confrontarsi direttamente con un testo di matrice europea, costringendoli ad abbandonare la mediazione dei legislatori locali e tutto ciò che essa comportava, ovvero il ricorso alle categorie giuridiche degli ordinamenti nazionali. Se questo è vero, è altresì vero che la disciplina comunitaria sulla responsabilità per il trattamento illecito dei dati presenta diverse lacune, ragion per cui i legislatori nazionali hanno dovuto ricostruire alcuni aspetti dell'art. 82 GDPR alla luce dei regimi di responsabilità locali[256].

La responsabilità ex art. 82 GDPR come responsabilità da inadempimento

Nell'ordinamento italiano, in vigenza della Direttiva, la responsabilità da trattamento illecito dei dati si configurava come una forma di responsabilità extracontrattuale; questo avveniva per due ordini di motivi: l'art. 15 Codice della privacy rimandava espressamente all'art. 2050 c.c.; il Codice della privacy non accennava minimamente all'ipotesi che il trattamento dei dati desse luogo a un rapporto obbligatorio fra le parti.

Come evidenziato, la lettura della responsabilità da trattamento illecito in senso extracontrattuale era principalmente legata alla formulazione dell'art. 15 Codice della privacy; pertanto, non stupisce che, alla sua abrogazione, la responsabilità *ex* art. 82 GDPR sia stata ricondotta nell'alveo della responsabilità contrattuale. Nello specifico, parte della dottrina interna ritiene che l'avvio di un trattamento dei dati comporti l'instaurazione di un vincolo obbligatorio fra *controller* e *processor,* da una parte, e *data subject,* dall'altra. Assumendo tale rapporto, l'inosservanza degli obblighi del GDPR da parte del titolare e del

[256]Vari aspetti della responsabilità da trattamento illecito dei dati non trovano una regolazione puntuale all'interno del GDPR, quali, ad esempio: i termini di prescrizione dell'azione risarcitoria e i limiti alla risarcibilità del danno (v. F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. Zorzi Galgano (a cura di), *Persone e Mercato dei Dati. Riflessioni sul GDPR*, Milano, Cedam, 2019, pp. 393 e ss.).

responsabile costituisce un inadempimento nei confronti dell'interessato, il quale ha diritto ad essere risarcito ai sensi dell'art. 82 GDPR. A sostegno della natura contrattuale della responsabilità in esame, la dottrina pone il ruolo che l'imputabilità assume sia nella norma comunitaria, sia nella disciplina nazionale della responsabilità da inadempimento. In quest'ultimo caso, l'imputabilità va intesa come la capacità del debitore di controllare gli eventi che potrebbero ostacolare l'adempimento dei suoi doveri comportamentali, al fine di soddisfare la pretesa creditoria[257]. Difatti, il debitore conosce, sin dall'inizio, il soggetto in favore del quale adempie alla propria obbligazione e i comportamenti da tenere per non ledere la sfera giuridica dello stesso. Parimenti, il *controller* e il *processor* sanno di obbligarsi verso l'interessato; all'opposto, il *data subject* potrebbe non sapere che i suoi dati sono oggetto di trattamento. Questo accade quando il trattamento ha fondamento nella legge, potendo il titolare prescindere dall'assenso del *data subject;* oppure*,* nell'ipotesi in cui il trattamento ha avuto inizio illecitamente, senza il consenso dell'interessato. Com'è noto, in tale eventualità il *data subject,* ha il diritto di opporsi al trattamento non appena ne venga a conoscenza.

Questa dottrina non ravvisa ostacoli nella configurazione della responsabilità contrattuale neppure quando sia un soggetto terzo a danneggiare l'interessato, sostenendo che sono il titolare e il responsabile ad essere gravati da un onere di protezione e, quindi, a dover impedire che si verifichino violazioni dei dati dell'interessato. In virtù di tale ragionamento, se vi fosse un *data brache* l'interessato potrebbe rifarsi tanto nei confronti del danneggiante, quanto nei confronti del *controller* e del *processor,* essendo questi venuti meno ai loro obblighi di protezione[258].

In conclusione, secondo il suesposto orientamento dottrinale, il trattamento dei dati da origine ad un rapporto obbligatorio; di conseguenza, la disciplina applicabile non può che essere quella della responsabilità da inadempimento, con tutte le implicazioni che ne derivano. Del resto, un simile inquadramento, lungi dal

[257]Sulle diverse posizioni assunte dalla dottrina in merito al concetto di imputabilità, v. G. Visintini, *Inadempimento e mora del debitore. Artt. 1218 -1222*, in *Commentario Schlesinger,* Milano, Giuffrè, 2006, pp. 94 e ss.

[258]Per riscontri di tale tesi nella letteratura italiana, v. F. Bilotta, *La responsabilità civile nel trattamento dei dati personali*, in R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 450 e ss.

limitarsi ad incidere sull'onere probatorio, ha effetti su tutti quegli aspetti che il Regolamento omette di disciplinare[259].

La responsabilità ex art. 82 GDPR come responsabilità ancipite

Alla tesi della responsabilità da inadempimento, se ne affianca una intermedia che considera la responsabilità da trattamento illecito dei dati, in parte, come una responsabilità contrattuale e, in parte, come una responsabilità extracontrattuale. La prima forma di responsabilità sarebbe ravvisabile solo laddove il danneggiante violasse un obbligo a lui imposto dal Regolamento; altrimenti, la responsabilità *ex* art. 82 GDPR sarebbe da ricondursi alla responsabilità aquiliana.

Prendendo in esame il meccanismo di imputazione di cui all'art. 82 GDPR, emerge che il titolare sarà chiamato a rispondere del danno solo quando il trattamento sia difforme dalle norme del Regolamento. Per quanto concerne il responsabile, invece, si configurano due fattispecie distinte, poiché questi sarà ritenuto responsabile, *in primis*, quando non adempia agli obblighi che il Regolamento gli rivolge specificatamente; *in secundis*, allorchè disattenda le istruzioni del *controller.* In relazione alle prime due ipotesi di responsabilità, ossia quella del titolare e la numero uno del responsabile, entrambi i soggetti sono gravati dall'obbligo *ex lege* di adempiere una prestazione nei confronti dell'interessato, il quale, a sua volta, ha il diritto di esigerla. Fra le parti si instaura un rapporto obbligatorio, che costituisce il presupposto della responsabilità contrattuale. Sussistendo tale presupposto, l'interessato, a fronte dell'inadempimento del titolare e del responsabile, potrà invocare la responsabilità *ex* art. 1218 c.c. Quanto alla seconda ipotesi, il *processor* non risponde dell'inadempimento nei confronti del *data subject*, poiché fra i due non esiste alcun vincolo obbligatorio. Al contrario, egli risponde del danno provocato contravvenendo alle istruzioni del *controller,* nell'ambito del rapporto instaurato con quest'ultimo. In tale scenario, viene a mancare il presupposto della responsabilità contrattuale, vale a dire il vincolo obbligatorio fra danneggiante e danneggiato; pertanto, la responsabilità del *processor* non può che essere inquadrata in quella extracontrattuale[260].

---

[259] V. nota 112.

[260]Così F. Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. Zorzi Galgano (a cura di), *Persone e Mercato dei Dati. Riflessioni sul GDPR*, cit. pp.394 e ss.

La responsabilità ex art. 82 GDPR come responsabilità extracontrattuale

Secondo altra parte della dottrina, gli oneri comportamentali del titolare e del responsabile non implicano l'esistenza di un rapporto obbligatorio con l'interessato, né consentono di qualificare la responsabilità come contrattuale. All'opposto, tali obblighi si inserirebbero nell'ambito della responsabilità extracontrattuale, per una duplice serie di ragioni. In primo luogo, la natura prevalentemente procedimentale degli oneri non conferisce all'interessato il diritto a una prestazione specifica, da parte del titolare o del responsabile, che soddisfi un suo interesse diretto. Ne deriva che non esiste alcun vincolo obbligatorio fra l'interessato e le altre parti dell'evento dannoso (il titolare e il responsabile); infatti, la relazione giuridica viene a costituirsi solo quando il danno sia effettivamente arrecato al *data subject*. In secondo luogo, ai sensi dell'art. 82 GDPR, la responsabilità di chi tratta i dati personali scaturisce dalla lesione di diritti e interessi fondamentali protetti a livello extracontrattuale[261], in particolare quello alla *data protection*[262].

Assumendo che la responsabilità da trattamento illecito dei dati sia di tipo extracontrattuale[263], questa dottrina si interroga su come essa si relazioni alla norma generale della responsabilità aquiliana, il 2043 c.c. Pur volendo attribuirle natura non contrattuale, appare evidente che questa responsabilità non può essere ricondotta *in toto* sotto l'art. 2043 c.c., specialmente se si considera il tipo di danni che un illecito trattamento dei dati può provocare. È ormai noto che la violazione dei dati personali può cagionare dei pregiudizi peculiari: spesso anonimi, molte volte "oscuri", nel senso che il danneggiato fatica a venirne a conoscenza, ancor più

[261]I suddetti interessi fondamentali sono espressamente richiamati all'art. 1 del GDPR.

[262]Sulla responsabilità da trattamento illecito dei dati come responsabilità *ex*tracontrattuale, v. M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro V. et al. (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1083 e ss.

[263]In merito a tale dottrina, occorre aggiungere che una parte dei suoi sostenitori rimane fedele all'orientamento maggioritario in vigenza dell'art. 15 Codice della privacy, vale a dire quello del criterio di imputazione oggettiva. Questi, infatti, aderiscono all'assunto per cui il concetto di rischio, centrale nel GDPR, è strettamente connesso alla responsabilità oggettiva; pertanto, qualificano la responsabilità di cui all' art. 82 GDPR come oggettiva. L'altra parte, invece, ritiene che la responsabilità del *controller* e/o *processor* debba essere letta alla luce del principio di *accountability*; dunque, non possa non essere concepita come una responsabilità aggravata per colpa presunta. Per un'analisi approfondita dei citati orientamenti dottrinali, v. D. Barbierato, *Trattamento dei dati personali e "nuova" responsabilità civile,* in *Responsabilità Civile e Previdenza,* 2019, n. 6, pp. 2156 e ss.

frequentemente "diffusi"[264]. Con tale espressione, si fa riferimento a quelle categorie di pregiudizi che non affliggono soltanto i diritti personali dei *data subject,* ma vanno a ledere interessi collettivi, ovvero appartenenti a intere categorie di soggetti, fino a colpire interessi propri di tutti i membri della società, quali quello alla liceità, alla trasparenza e alla correttezza del trattamento. Dinnanzi a siffatte tipologie di danni, anche le esigenze di tutela sono cambiate. Benché il trattamento dei dati porti dei benefici economici alla comunità, essendo i dati diventati <<materia prima di indubbio valore>>[265], esso incide negativamente sulla tutela dei diritti fondamentali della collettività, spesso sacrificati a favore di logiche di mercato. Da qui, il bisogno di risanare un danno che non è più del singolo individuo, ma di molti, se non di tutti[266].

In un contesto del genere, il tradizionale sistema di responsabilità aquiliana mostra tutti i suoi limiti, essendo costruito sull'idea, ormai superata, che a un autore del danno corrisponda un solo danneggiato. L'inadeguatezza del sistema non deve spingere a ripensare l'inquadramento della responsabilità da illecito trattamento dei dati, poiché questa resta una responsabilità extracontrattuale. Tuttavia, rispetto al modello dell'art. 2043 c.c., tale responsabilità deve essere considerata una forma autonoma e speciale[267].

---

[264]Sulle forme più comuni di violazione dei dati personali, v. D. Barbierato, *Dati personali e Internet*, Napoli, Edizioni Scientifiche Italiane, 2008, pp. 11 e ss., la quale, fra le principali fonti di pericolo per i dati, annovera: l'accettazione dei *cookies*, cioè strumenti tramite i quali i titolari di siti *web* entrano in possesso di informazioni personali degli utenti; la presenza sulle pagine internet di *web bug*, ossia immagini che consentono di catturare notizie sui visitatori dei siti *web* per divulgarli a soggetti terzi, o ancora la pubblicazione *online* di notizie altrui in modo anonimo.

[265]Cfr. Zeno Zencovich, A. Zoppini, *La disciplina dei servizi telematici nel quadro delle proposte comunitarie di tutela dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 1992, n. 3, p.773.

[266]Sin dai primi commenti al Regolamento, la dottrina aveva evidenziato che una tutela a carattere individuale era insufficiente per proteggere gli interessati. In questo senso, v. A. Mantelero, *Responsabilità e rischio nel Reg. UE 679/2016*, in *Le nuove leggi civili commentate*, 2017, n. 1, pp. 152 e ss, il quale ritiene che la ragione per cui si è adottato un approccio individualista risiede <<nel fatto che il diritto alla protezione dei dati è strutturalmente concepito come diritto individuale>>. Infatti, <<è vero che la dimensione sociale dello stesso è stata considerata dalle corti ed è alla base della disciplina adottata in materia>>, ma è <<al titolare del diritto che si guarda principalmente in termini di tutela ed attivazione della stessa>>.

[267]In questi termini, v. M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro V. et al. (a cura di), *I dati personali nel diritto europeo*, cit., pp. 1088 e ss.

3.2. La responsabilità *ex* art. 82 GDPR, una responsabilità autonoma e speciale

Le conclusioni raggiunte dall'ultimo orientamento analizzato appaiono condivisibili; diversamente, non si comprende perché questo tenti di ricondurre la responsabilità da trattamento illecito dei dati nelle categorie dell'ordinamento giuridico nazionale. D'altronde, se si afferma che la responsabilità *ex* art. 82 GDPR è una responsabilità autonoma e speciale rispetto alle altre, essa deve essere interpretata indipendentemente dalla disciplina dei singoli Stati. Ciò implica che, laddove si voglia intentare un'azione risarcitoria a seguito di un trattamento illecito dei dati, questa debba essere avviata sulla base dell'art. 82 GDPR e non dell'art. 2043 c.c., o di equivalenti disposizioni di altri ordinamenti europei. Solo discostandosi dagli schemi giuridici nazionali, l'art. 82 GDPR può essere interpretato in maniera uniforme dai legislatori europei, così che gli Stati membri possano garantire un eguale livello di protezione dei dati all'interno dell'Unione. Nello specifico, è auspicabile che si affermi al più presto una lettura omogenea degli aspetti sui quali il GDPR risulta meno chiaro, giacché sono questi ad alimentare il dibattito nella dottrina e giurisprudenza locale. Si pensi, ad esempio, al danno immateriale, la cui risarcibilità è oggetto di discussione nell'ordinamento italiano, così come nel resto d'Europa. Ebbene, è fondamentale che sia definito uno standard europeo in proposito, poiché il risarcimento del danno immateriale è imprescindibile per assicurare l'effettività della tutela sancita dal Regolamento[268].

Per una lettura uniforme dell'art. 82 GDPR, la norma deve essere interpretata in modo sistematico e teleologico, tenendo quindi conto dei principi, delle disposizioni legislative e delle pronunce giurisprudenziali dell'Unione. Una volta formulate le linee guida interpretative a livello europeo, l'art. 82 GDPR va applicato nei diversi Stati membri. Questo deve avvenire alla luce delle succitate linee guida, senza però che si generi un contrasto con i principi giuridici nazionali[269].

---

[268]Così D. De Rada, *La responsabilità civile per illecito trattamento dei dati ex art. 82 GDPR*, Santarcangelo di Romagna, Maggioli Editore, 2023, pp. 68 e ss.

[269]Tale risultato può essere ottenuto tramite l'adozione di una normativa nazionale che incorpori, al suo interno, le norme del Regolamento. Sul punto, v. E. O'Dell, *Compensation for Breach of the General Data Protection Regulation*, in *Dublin University Law Journal (ns,)* vol. XL, 2017, n.1, pp. 21 e ss., il quale riporta l'esempio dell'Irlanda, nella cui legislazione è stato interamente trasposto il testo dell'art. 82 GDPR.

Eppure, fino a questo momento i giudici nazionali non sembrano aver adottato l'approccio sperato. Al contrario, si sono sviluppate interpretazioni spesso in disaccordo tra di loro, soprattutto riguardo alla risarcibilità del danno immateriale e alla quantificazione del risarcimento[270].

3.2.1. Uno sguardo alla giurisprudenza europea sul danno immateriale

La giurisprudenza tedesca

Quanto all' Europa, la prima richiesta di risarcimento per danni immateriali, *ex* art. 82 GDPR, è stata avanzata dinanzi al Tribunale di Diez, il 7 novembre 2018[271]. Su una pretesa analoga, si è successivamente espresso il Tribunale regionale superiore di Dresda[272]. Nel caso esaminato da quest'ultima pronuncia, il ricorrente lamentava di aver subito dei danni immateriali a seguito dell'eliminazione di un suo "post" da parte del convenuto, un *social network provider*, che, dopo la cancellazione del contenuto, aveva sospeso l'*account* dell'attore per tre giorni. Il Tribunale di Dresda ha respinto la pretesa risarcitoria, ritenendo che i requisiti dell'art. 82, par. 1, GDPR non fossero soddisfatti. Innanzitutto, il Tribunale ha stabilito che né l'eliminazione del "post", né la sospensione dell'*account* costituivano una violazione delle disposizioni obbligatorie del GDPR, giacché le azioni del *provider* erano giustificate dal consenso espresso dal ricorrente al momento dell'accettazione dei termini d'uso. Inoltre, il Tribunale ha affermato che la sospensione dell'*account* non configurava un danno ai sensi dell'art. 82 GDPR, perché questa era solo una violazione "minore" del Regolamento; mentre, per essere risarcibile, il danno da inosservanza del GDPR deve essere rilevante. A parere del Tribunale, non può essere accolta la pretesa di un ricorrente che abbia percepito un disagio solo soggettivamente, senza subire una seria compromissione della propria immagine o reputazione. Altrimenti, si assisterebbe ad un accoglimento incondizionato di richieste di risarcimento. Da ultimo, il Tribunale ha fornito un esempio di un danno immateriale rilevante, affermando che sarebbe risarcibile il pregiudizio derivante da una violazione del

[271]Tribunale locale di Diez, 7 novembre 2018, n. 8 C 130/18, disponibile *online* su https://openjur.de/u/2116788.html.
[272] Tribunale regionale superiore di Dresda, 11 giugno 2019, n. 4 U 760/19, disponibile *online* su https://openjur.de/u/2316062.html.

GDPR, allorchè questa coinvolga un gruppo omogeneo di persone e rappresenti una forma di commercializzazione deliberata, illegale e su larga scala.

Benché il Tribunale abbia finalmente accennato a dei criteri per identificare il danno risarcibile, in particolare il fattore della "commercializzazione", è indubbio che residui ancora un certo grado di incertezza giuridica. Invero, il Tribunale non ha chiarito quali violazioni del Regolamento siano da qualificarsi come bagatellari e quali no[273].

Neppure le successive pronunce giurisprudenziali hanno fornito chiarimenti in materia, limitandosi a ribadire che l'art. 82 GDPR permette di superare l'approccio nazionale sul danno immateriale, il quale richiede la prova di una violazione grave, senza tuttavia rendere automatico il risarcimento di tali danni[274]. Affinché questi siano risarciti, deve comunque essere dimostrata una seria lesione dei diritti personali.

Nonostante l'orientamento citato sia quello prevalente, nella giurisprudenza tedesca sta lentamente emergendo una tendenza opposta. Esemplificativa, in tal senso, la decisione del Tribunale di Monaco su un furto di dati seguito ad un *hackeraggio*[275]. In questo caso, il Tribunale ha riconosciuto l'esistenza di un danno immateriale, condannando il convenuto al risarcimento non solo del danno presente, ma anche dei danni futuri. A sorprendere, oltre al riferimento ai danni futuri, è l'accoglimento della richiesta risarcitoria in sé; difatti, non vi era alcuna evidenza che l'*hacker*, dopo aver sottratto i dati del ricorrente, li avesse usati in modo illecito. La pronuncia, dunque, si pone in netto contrasto con il filone giurisprudenziale che richiede *in primis* la prova del danno, *in secundis* che questo sia notevole.

---

[273] Per un commento alla pronuncia del Tribunale regionale superiore di Dresda, v. S. Schonhofen, F. Wilde-Detmering, A. Hardinghaus, *German court ruling: no claims for damages under Article 82 GDPR for minor GDPR violations*, 21 agosto 2019, disponibile *online* su https://www.technologylawdispatch.com/2019/08/in-the-courts/german-court-ruling-no-claims-for-damages-under-article-82-gdpr-for-minor-gdpr-violations/.

[274]Tribunale regionale di Karlsruhe, 2 agosto 2019, n. 8 O 26/19. In merito, v. *LG Karlsruhe: Kein Schadensersatz-Anspruch nach der DSGVO aus generalpräventiven Gründen*, 5 novembre 2019, disponibile *online* su https://www.dr-bahr.com/news/kein-schadensersatz-anspruch-nach-der-dsgvo-aus-generalpraeventiven-gruenden.html.

[275]Tribunale regionale di Monaco I, 7 novembre 2019, n. 34 O 13123/19, disponibile *online* su https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2019-N28276?hl=true&fontsize=small.

La giurisprudenza austriaca

Passando alla giurisprudenza austriaca, si osserva che le corti nazionali, investite da ricorsi per risarcimento di danni immateriali ai sensi dell'art. 82 GDPR, hanno adottato un approccio analogo a quello tedesco. Ciò trova conferma nella decisione del Tribunale regionale superiore di Innsbruck[276], il quale ha ribaltato la pronuncia di primo grado del Tribunale regionale di Feldkirc, dell'agosto 2019[277]. In prima istanza, il Tribunale aveva riconosciuto al ricorrente di aver subito dei danni immateriali derivanti dal trattamento illecito dei propri dati sensibili; pertanto, aveva accolto la sua richiesta risarcitoria. In secondo grado, invece, il Tribunale ha negato che l'attore avesse dato prova di tali danni, annullando la precedente pronuncia. A sostegno della sua decisione, il Tribunale ha posto il principio per cui una violazione del GDPR non può essere automaticamente associata a un danno immateriale, ma occorre che questa leda la sfera emotiva del ricorrente. Ancora, il Tribunale ha precisato che l'intensità del pregiudizio assume un ruolo centrale nella determinazione del danno; infatti, è necessario che la lesione della sfera personale raggiunga un certo livello di gravità per integrare un danno immateriale[278].

Al pari di quella tedesca, la giurisprudenza austriaca condiziona il risarcimento del danno immateriale alla dimostrazione della sua effettiva esistenza e al carattere non bagatellare dello stesso.

La giurisprudenza olandese

Un approccio differente è stato adottato dalle corti olandesi, che appaiono meno restie a riconoscere l'esistenza, e quindi la risarcibilità, del danno immateriale da trattamento illecito di dati.

Il Tribunale distrettuale di Overijssel, ad esempio, ha ritenuto che il ricorrente avesse subito un danno immateriale quando l'azienda per cui lavorava

---

[276] Tribunale regionale superiore di Innsbruck, 13 febbraio 2020, n. 1 R 182/19b, disponibile *online* su https://www.dataprotect.at/2020/03/06/post-schadenersatz/.

[277] Tribunale regionale di Feldkirch, 14 agosto 2019, n. 57 Cg 30/19b, disponibile *online* su file:///C:/Users//Downloads/Urteil-LG-Feldkirch-O%CC%88sterreichische-Post-AG-anonymisiert-online%20(4).pdf. Per un commento, v. T. Schweiger, *Die Post bringt allen was .... oder: „es stört mich, dass meine Daten verarbeitet werden."*,11 ottobre 2019, disponibile *online* su https://www.dataprotect.at/parteienaffinit%C3%A4t-und-schadenersatz/.

[278] Il Tribunale regionale superiore di Innsbruck fornisce alcuni criteri per valutare la serietà della lesione; in particolare, menziona la tipologia di dati coinvolti, la gravità e la durata della violazione, nonché l'eventuale trasferimento di dati a soggetti terzi.

aveva divulgato i suoi dati personali a soggetti esterni, senza il suo consenso[279]. Il Tribunale ha accolto la pretesa risarcitoria sulla base di una lettura congiunta dell'art. 82 GDPR e dell'art. 6:106 del codice civile olandese, inaugurando un vero e proprio filone giurisprudenziale: per la prima volta, veniva richiamato il criterio di equità, di cui all'art. 6:106 c.c.[280], in materia di trattamento illecito di dati.

Sulla scia del caso di Overijssel, il Tribunale distrettuale di Amsterdam ha affermato che il concetto di danno va inteso in senso ampio; ragion per cui, non è necessario che il pregiudizio immateriale sia rilevante per essere risarcito[281]. Secondo il Tribunale, è sufficiente che il ricorrente dimostri di aver subito quel tipo di danno, dovendo poi essere applicato il criterio di equità di cui all'art. 6:106 c.c. per individuare il *quantum* risarcitorio.

Al pari di quella di Amsterdam, altre corti locali hanno sostenuto la risarcibilità del danno immateriale a prescindere dalla sua gravità, richiamando il principio nazionale di equità[282]. In questo modo, la giurisprudenza olandese ha fatto un passo in avanti sulla risarcibilità *ex* art. 82 GDPR del danno immateriale. Ciononostante, va sottolineato che i risarcimenti concessi dai giudici dei Paesi Bassi sono sempre stati di importo modesto. Nel caso del Tribunale di Overijssel, il danno è stato quantificato in 500 euro; in quello del Tribunale di Amsterdam, in appena 250 euro.

La giurisprudenza italiana

Le corti olandesi non sono le uniche ad aver abbandonato il criterio della gravità del danno; difatti, in una recente pronuncia, la Corte di Cassazione italiana ha raggiunto la medesima conclusione, discostandosi dalla consolidata giurisprudenza nazionale in materia di danno da trattamento dei dati personali[283].

---

[279]Tribunale distrettuale di Overijssel, 28 maggio 2019, n. AK_18_2047, disponibile *online* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBOVE:2019:1827.

[280]L'art. 6:106 codice civile olandese enuncia il criterio di equità, disponendo che <<*the injured person has a right of compensation for damage that does not consist of material loss, assessed in conformity with the standards of reasonableness and fairness*>>.

[281]Tribunale distrettuale di Amsterdam, 2 settembre 2019, n. 7560515 CV ESPL 19-4611, disponibile *online* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2019:6490.

[282]Tribunale distrettuale di Noord-Nederland, 15 gennaio 2020, n. C/18/189406/HA SAB 19-6, disponibile *online* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNNE:2020:24, il quale osserva che il legislatore nazionale, nel redigere l'art. 6:106 del codice civile olandese, ha riconosciuto al giudice ampia discrezionalità nella valutazione del danno immateriale; pertanto, il Tribunale non è vincolato alle normali regole dell'obbligo di dichiarazione e dell'onere della prova.

[283]Cass. 12 maggio 2023, n. 13073, in *Nuova giur. civ. comm.*, 2023, V, p. 1125, con nota di G.M. Riccio*, Dati personali e rimedi: diritti degli interessati e profili risarcitori*.

In passato, la Suprema Corte aveva sostenuto che il danno non patrimoniale da violazione dei dati personali poteva essere risarcito solo laddove la lesione fosse stata seria e il danno grave[284]. D'altro canto, il diritto alla *data protection* non era esente dal bilanciamento con il principio di solidarietà di cui all'art. 2 della Costituzione[285], in virtù del quale un pregiudizio di lieve entità non dovrebbe essere risarcito, bensì tollerato[286].

I giudici territoriali, d'altro canto, si sono generalmente allineati a tali argomentazioni quando hanno dovuto pronunciarsi sulle richieste di risarcimento per danni immateriali. A mero titolo esemplificativo, si pensi al caso affrontato dal Tribunale di Reggio Calabria sulla pubblicazione di immagini senza il consenso dell'interessato sul servizio "*Street View*" di Google. Il Tribunale adito ha dapprima ribadito la necessità che fosse dimostrato il danno conseguenza, per poi precisare che il pregiudizio non può consistere in un mero fastidio, dovendo questo eccedere la normale tollerabilità[287].

Tuttavia, il suddetto orientamento appare superato dalla pronuncia di Cassazione in esame. Quest'ultima prende le mosse dal caso di un dipendente comunale che, per errore, aveva pubblicato i dati relativi a un pignoramento gravante su un'altra dipendente, la quale aveva lamentato la violazione dei propri dati personali e avanzato una pretesa risarcitoria al Comune. Dinnanzi a tale istanza, sia il Tribunale di primo grado, che la Corte d'Appello avevano ammesso la responsabilità dell'ente convenuto, condannandolo al risarcimento del danno non patrimoniale. Il Comune, allora, aveva presentato ricorso in Cassazione, ove era stato confermato quanto già stabilito in appello, ossia che il danno non patrimoniale da violazione dei dati personali derivava dalla lesione del diritto fondamentale alla

---

[284]Cass. 20 agosto 2020, n. 17383, in *Dir. Internet*, 2020, 619, con nota di A. Avitabile, *Il risarcimento del danno a seguito dell'illecito trattamento di dati personali: un nuovo impulso dal reg. UE 27 aprile 2016 n. 679.*

[285] Cass. 11 gennaio 2016, n. 222, in *Dir. e giust.,* 2016, 12, con nota di M. Alovisio, *Risarcimento del danno per diffusione indebita di dati sanitari.*

[286]Cass. 15 luglio 2014, n. 16133, in *Danno e resp.,* 2015, 339*,* con note di V. Ceccarelli, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*; M. Nitti, *La valutazione della "gravita` della lesione" e della "serieta` del danno" nel risarcimento del danno non patrimoniale da violazione della privacy.*

[287]Tribunale di Reggio Calabria, 25 febbraio 2020, con commento di A. Souihel, V. Zanni, *Risarcimento danni privacy: l'Ue allarga le maglie, l'Italia resta cauta*, settembre 2024, disponibile *online* su https://www.agendadigitale.eu/sicurezza/privacy/risarcimento-danni-privacy-lue-allarga-le-maglie-litalia-resta-cauta/.

data protection, sancito a livello costituzionale. Inoltre, la Corte aveva aggiunto che il danneggiato <<può ottenere il risarcimento di qualunque danno occorsogli, anche se la lesione sia marginale>>[288]. Si assiste, dunque, ad un "cambio di rotta" della Suprema Corte, che pare aver superato l'idea per cui un danno da violazione dei dati debba necessariamente essere grave per essere risarcibile.

A riguardo, è opportuno sin d'ora osservare che, solo qualche giorno prima, la Corte di Giustizia, con una pronuncia di cui si dirà meglio in seguito, era pervenuta a conclusioni non lontane da quelle dell'ordinanza in commento.

Riflessioni conclusive sulla produzione giurisprudenziale europea

Dal confronto delle succitate pronunce giurisprudenziali, si evince che non esiste un approccio europeo uniforme sulla risarcibilità del danno immateriale, in quanto le corti nazionali spesso raggiungono delle conclusioni radicalmente opposte tra di loro. La conseguenza di questa disomogeneità è che, al momento, gli Stati membri sono incapaci di assicurare una protezione concreta ai danneggiati, e non solo. L'incertezza interpretativa che caratterizza la materia non pregiudica solo questa categoria di soggetti, ma anche gli attori del trattamento, ovvero coloro nei confronti dei quali i primi agiscono in giudizio.

Ebbene, in un contesto simile, appare ragionevole supporre che la Corte di Giustizia sarà chiamata a intervenire per promuovere un'interpretazione uniforme della tutela risarcitoria *ex* art. 82 del GDPR[289].

3.2.2. Le criticità della responsabilità *ex* art. 82 GDPR al vaglio della Corte di Giustizia: il caso UI contro *Österreichische Post AG*

Com'era facile prevedere, non è passato molto tempo dall'entrata in vigore del GDPR che la Corte di Lussemburgo ha dovuto chiarire aspetti fondamentali per l'applicazione della disciplina sulla responsabilità da trattamento illecito dei dati da parte dei giudici nazionali.

In particolare, la vicenda che ha determinato il ricorso alla Corte di Giustizia ha avuto origine in Austria, dove un cittadino, identificato come "UI", lamentava di essere stato erratamente associato a un partito da un'azienda locale, la

[288] Cass., 12 maggio 2023, n. 13073, cit., par. 5.
[289] Su posizioni simili, v. De Rada, *La responsabilità civile per illecito trattamento dei dati ex art. 82 GDPR*, cit., pp. 69 e ss.

"*Österreichische Post"*, la quale raccoglieva informazioni sulle affinità politiche della popolazione, per poi venderle a soggetti terzi. Ebbene, tale associazione, inesatta e priva di fondamento, avrebbe provocato nel ricorrente un sentimento di umiliazione e di dispiacere. Pertanto, egli domandava al Tribunale distrettuale di Vienna che l'azienda cessasse il trattamento dei suoi dati personali e lo risarcisse per il danno immateriale subito. Nel luglio 2020, il Tribunale accoglieva la domanda inibitoria, respingendo quella risarcitoria. Tale decisione veniva altresì confermata in sede di appello, poiché la Corte riteneva che le emozioni negative del ricorrente non fossero idonee ad integrare un danno risarcibile ai sensi della legge nazionale, la quale richiedeva che fosse provata la gravità del danno[290].

Successivamente, veniva adita la Corte Suprema austriaca, la quale però dichiarava il ricorso inammissibile, sospendendo il caso e rimettendolo alla Corte di Giustizia dell'Unione Europea[291]. A quest'ultima venivano sottoposte le seguenti questioni: se sia sufficiente una semplice violazione del GDPR per ottenere un risarcimento; se esistano prescrizioni europee diverse dall'equivalenza e l'effettività per quantificare il danno risarcibile; se l'applicazione della soglia di gravità della lesione al risarcimento da danno immateriale sia compatibile con il diritto europeo.

Alla luce dei quesiti posti, occorre preliminarmente rilevare come la pronuncia in esame, malgrado abbia generato delle perplessità nella dottrina europea, rappresenti un momento di svolta per la tutela dei dati personali, specie per quanto riguarda il risarcimento dei danni immateriali derivanti dalla violazione del GDPR. Infatti, la Corte di Giustizia ha affermato che l'espressione "danno immateriale" deve essere interpretata in modo autonomo e uniforme

---

[290]Per un'analisi approfondita sull'*iter* processuale che ha preceduto il ricorso alla Corte di Giustizia, v. A. Lottini, *Risarcimento del danno immateriale a seguito della violazione del regolamento (UE) 2016/679: la sentenza* Österreichische Post *determina un cambio di paradigma?,* in *Quaderni AISDUE*, 2023, n. 2, pp. 187 e ss.

[291]Corte di Giustizia dell'Unione Europea, 4 maggio 2023, C-300/21, *UI v.* Österreichische Post AG, in *Foro it.*, 2023, IV, 268 ss., con note di A. Palmieri, R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, c. 278 e ss.; S. Pagliantini, *Un altro palcoscenico della "guerra" tra le corti: il danno (immateriale) bagatellare dell' art. 82 Gdpr* c. 285 e ss.; M. Federico, *"La tempesta perfetta": ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva*, c. 293 ss.; in *Nuova g. civ. comm.*, 2023, pp. 1119 e ss., con commento di G. Calabrese, *Il danno da "perdita di controllo dei dati personali" nel pensiero della Corte di Giustizia UE*; nel medesimo fascicolo, alla sentenza sono dedicati, inoltre, i contributi di C. Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, pp. 1136 e ss.; C. Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, pp. 1150 e ss.

nell'ordinamento europeo, senza che sia fatto alcun riferimento alle normative nazionali. Ciò, a parere della Corte, sarebbe coerente con l'obiettivo del GDPR di garantire una protezione omogenea in tutta l'Unione[292].

Passando al contenuto della pronuncia, e nello specifico al quesito sull'inosservanza del Regolamento quale presupposto per il risarcimento, la Corte di Giustizia ha affermato che il danno è risarcibile allorchè ricorrano tre condizioni, ovvero una violazione del GDPR, l'esistenza di un danno, ed infine un nesso causale tra la violazione e il danno subito. Dunque, la mera inosservanza del Regolamento non è sufficiente ad ottenere il risarcimento. D'altronde, se la violazione della normativa fosse, da sola, in grado di assicurare la spettanza del risarcimento, il legislatore non avrebbe fatto espresso riferimento al danno, giacché questo avrebbe rappresentato un'inutile ripetizione[293].

Quanto all'ammontare del risarcimento, la Corte ha rilevato che, in assenza di disposizioni dell'Unione volte a determinarlo, non possono non essere applicate le norme di diritto interno; ciò nonostante, devono essere comunque rispettati i principi comunitari di equivalenza ed effettività della tutela[294].

Rispetto alla soglia di gravità della lesione, invece, la Corte ha ritenuto che limitare la risarcibilità del danno immateriale a tale parametro avrebbe contraddetto gli scopi del GDPR, compromettendo la protezione dei dati personali e l'applicazione uniforme della normativa europea[295]. Invero, secondo la Corte, fissare una soglia di gravità del danno comporterebbe un'eccessiva discrezionalità dei giudici nazionali nell'accoglimento delle richieste risarcitorie, il che condurrebbe a divergenze nell'interpretazione e nell'attuazione del GDPR[296].

Proprio in relazione a quest'ultimo enunciato, letto unitamente alla risposta della Corte al primo quesito, si sono sviluppate le principali critiche dottrinali. Del resto, parte della dottrina non ha potuto non sottolineare che, se da un lato la Corte

---

[292]Corte di Giustizia dell'Unione Europea, *op. ult. cit.,* par. 44.
[293]Corte di Giustizia dell'Unione Europea, *op. ult. cit.,* par. 34.
[294]Corte di Giustizia dell'Unione Europea, *op. ult. cit.,* par. 54.
[295]In questo senso anche Corte di Giustizia dell'Unione Europea, 25 gennaio 2024, C-687/21*, BL contro* MediaMarktSaturn Hagen-Iserlohn GmbH, disponibile *online* su https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62021CJ0687, la quale ha affermato che <<poiché il diritto al risarcimento previsto all'articolo 82, paragrafo 1, del RGPD non svolge una funzione dissuasiva, né punitiva, ma svolge una funzione compensativa, la gravità della violazione di tale regolamento che ha causato il danno di cui trattasi non può incidere sull'importo del risarcimento concesso in base a detta disposizione>>.
[296]Corte di Giustizia dell'Unione Europea, 4 maggio 2023, C-300/21, cit.*,* par. 49.

ha escluso la configurabilità di un danno *in re ipsa* anche quando la violazione del GDPR incide su un diritto fondamentale, nel caso di specie il diritto all'identità politica, non potendo prescindersi dalla prova di un danno conseguenza; dall'altro, essa ha negato che i giudici nazionali possano stabilire una soglia di gravità del danno, finendo così per ammettere la risarcibilità di danni bagatellari. In sostanza, << la Corte di giustizia toglie con la sinistra, là dove impone all'attore di fornire la prova del danno (senza che sia possibile invocare la "sacredness" del valore costituzionale inciso), e s'ingegna di ridare con la destra, disinnescando qualsiasi filtro, inteso […] a intercettare pretese volatili e ricattatorie>>[297].

Altrettanti dubbi hanno suscitato le affermazioni dei giudici di Lussemburgo rispetto alla seconda questione. Difatti, benché abbia richiamato i principi di equivalenza ed effettività per definire l'importo del risarcimento, la Corte non ha fornito dei criteri specifici per calcolare l'entità dei danni derivanti dalla lesione ai dati personali[298].

In conclusione, dalle precedenti considerazioni emerge come tale pronuncia, seppur di indiscutibile rilevanza, abbia lasciato ampi margini di libertà ai giudici nazionali nel valutare l'accoglimento delle richieste risarcitorie per violazione del GDPR, nonché l'ammontare dei danni risarcibili. Dunque, la Corte non sembra essere riuscita ad arginare le discrepanze interpretative tra gli Stati membri in materia di danni immateriali.

4. La responsabilità solidale degli attori del trattamento

Nell'intento di garantire maggior tutela al danneggiato, l'art. 82, par. 4, GDPR fissa un regime di responsabilità solidale tra tutti coloro che abbiano preso parte al trattamento causativo del danno[299]. In virtù di tale regime, titolari, contitolari e responsabili del trattamento divengono congiuntamente responsabili nei confronti dell'interessato. Diversamente, la norma non menziona né la figura

[297]A. Palmieri, R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, cit., par. 4.
[298]G. Calabrese, *Il danno da "perdita di controllo dei dati personali" nel pensiero della Corte di Giustizia UE*, cit., par. 4.
[299]Ai sensi dell'art. 82, par. 4, GDPR << qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano […] responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato>>.

del sub-responsabile, né quella *Data Protection Officer*, della cui esclusione si dirà meglio in seguito.

L'art. 82 GDPR, però, non si limita a prevedere la responsabilità solidale dei partecipanti al trattamento, ma dispone altresì che, nei rapporti interni, sia valutato l'effettivo contributo causale di ciascuno alla realizzazione del danno[300]. Di conseguenza, colui che abbia risarcito integralmente il danno potrà rivalersi sugli altri titolari e/o responsabili, esercitando un'azione di regresso o surroga.

4.1. Titolarità congiunta del trattamento e responsabilità solidale

Tra i responsabili in solido, il GDPR individua i contitolari del trattamento, volendo, con tale espressione, riferirsi all'ipotesi in cui due o più *controller* determinino congiuntamente le finalità e i mezzi del trattamento dei dati personali. D'altronde, il coinvolgimento di più titolari si spiega alla luce della pluralità di attività che concorrono a formare il trattamento, le quali rendono difficile per un solo *controller* gestire l'operazione[301]. Tuttavia, non è sempre agevole comprendere quando più *controller* siano anche *joint controllers*. Per chiarire questo aspetto, la Commissione Europea ha fornito un esempio di contitolarità, descrivendo la situazione in cui un'azienda offre servizi di *babysitting* tramite una piattaforma *online* e si avvale di un'altra società per fornire prestazioni aggiuntive, erogate attraverso la stessa piattaforma. In tal caso, le aziende utilizzano un unico portale per entrambi gli scopi, condividendo i dati dei loro clienti. Le due sono contitolari del trattamento, poiché ne condividono sia le finalità, che i mezzi: non solo concordano di offrire servizi combinati, ma progettano e utilizzano una piattaforma comune[302].

---

[300]Ai sensi dell'art. 82, par. 5, GDPR <<qualora un titolare del trattamento o un responsabile del trattamento abbia pagato […] l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno>>.

[301]Così Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"* (WP 169), cit., par. 3.1. lett. d, il quale precisa che la partecipazione dei contitolari alla determinazione congiunta può assumere forme diverse e non è necessario che sia equamente condivisa. Infatti, in caso di una pluralità di attori, questi possono avere una relazione molto stretta (condividendo tutte le finalità e i mezzi del trattamento); oppure, una relazione più debole (condividendo, alternativamente, le finalità o i mezzi, o solo una parte di essi).

[302]Cfr. Commissione Europea, *What is a data controller or a data processor?,* disponibile *online* su https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controllerprocessor/what-data-controller-or-data-processor_en.

Una volta chiarito il concetto, è opportuno soffermarsi sulla fonte della contitolarità, in quanto tale rapporto può sorgere dalla volontà, di due o più titolari, di disporre comunemente di dati relativi al medesimo interessato: quindi, da un accordo (d'ora in avanti, accordo esterno, per distinguerlo dall'accordo interno di cui all'art. 26 GDPR). Altrimenti, da un obbligo di natura legislativa o comunque derivante da un atto giuridicamente vincolante[303]. La diversa origine della contitolarità incide altresì sull'accordo interno di cui all'art. 26 GDPR; difatti, se il rapporto si basa sulla volontà negoziale delle parti, l'accordo interno attua quello esterno, dettando le regole per lo svolgimento del trattamento congiunto. Laddove, invece, la relazione di contitolarità abbia fondamento nella legge, anche l'accordo interno deve rifarsi al dettato normativo, risultando maggiormente vincolato nel contenuto[304].

Rispetto a quanto osservato, è importante sottolineare che una volta sola si è fatto rimando al Regolamento, ed era in relazione all'accordo interno; ciò dipende dal fatto che il GDPR non disciplina le fonti della contitolarità, ma, una volta instaurato il legame fra i titolari, impone loro di stipulare un accordo interno ai sensi dell'art. 26 GDPR. Tale disposizione rappresenta il riferimento principale per i *controller* che intendano concludere l'accordo, giacché non sono molti gli Stati membri ad aver regolato la materia a livello nazionale. In particolare, la legge sulla protezione dei dati che si sofferma maggiormente sulla contitolarità è quella belga, la quale vi dedica un articolo *ad hoc*[305]. È indubbio che un simile vuoto normativo comporti delle difficoltà per i contitolari, essendo questi privi di linee guida circa i requisiti dell'accordo interno. Ad ogni modo, il suo contenuto essenziale può essere

---

[303]Circa il fondamento della contitolarità, v. Garante della protezione dei dati delle istituzioni dell'Unione Europea (EDPS), *EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725*, 7 novembre 2019, pp. 27 e ss., disponibile *online* su https://www.edps.europa.eu/sites/default/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf, il quale ha elaborato delle linee guida sul Regolamento n. 45 del 2011, ovvero l'atto normativo attuativo del GDPR nell'ambito delle istituzioni europee.

[304]Sul nesso tra le fonti della contitolarità e la struttura dell'accordo interno, v. F. Pizzetti, L. Greco, *Commento all'art. 26 Reg. 679/2016,* in R. D'Orazio et al. (a cura di), *Codice della Privacy e Data Protection,* Milano, Giuffrè, 2021, pp. 434 e ss.

[305]La legge belga sulla protezione dei dati, entrata in vigore il 30 luglio 2018, regola la figura del contitolare del trattamento ai sensi dell'art. 52. Esso dispone che due o più titolari debbano considerarsi contitolari allorchè decidano insieme finalità e mezzi del trattamento. Ancora, la norma sancisce che le rispettive responsabilità, specialmente riguardo ai diritti dell'interessato, siano definite da un accordo, salvo che non siano già stabilite da norme o accordi internazionali. A proposito della legge belga sulla protezione dei dati, v. *Data protection laws of the world. Belgium,* 6 febbraio 2024, disponibile *online* su https://www.dlapiperdataprotection.com/index.html?t=law&c=BE.

ricostruito grazie all'art. 26 GDPR. Quest'ultimo stabilisce che le clausole dell'accordo debbano, prima di tutto, esplicitare i doveri di informazione dei contitolari nei confronti degli interessati[306]. Ancora, l'art. 26 GDPR invita i contitolari ad una chiara allocazione delle responsabilità derivanti dal Regolamento, anche in relazione alla supervisione e alle misure delle autorità di controllo[307].

Dall'analisi dell'art. 26 GDPR, emerge che i contitolari del trattamento hanno una certa discrezionalità nell'attribuzione delle responsabilità. Del resto, la norma non menziona esplicitamente un regime di responsabilità solidale, contrariamente a quanto indicato nella versione preliminare del Regolamento. Se questo è vero, è altrettanto vero che il GDPR richiama il principio di solidarietà all'art. 82, par. 4, GDPR, riguardo il risarcimento degli interessati. L'articolo dispone che, qualora più titolari siano coinvolti nello stesso trattamento, e ne derivi un danno, ciascuno di essi è solidalmente responsabile per l'intero ammontare, così da garantire un risarcimento effettivo al *data subject*.

Inoltre, il Regolamento, pur non facendone menzione all'art. 26 GDPR, evoca il principio di solidarietà sia al considerando 146, che all'art. 82, par. 5, GDPR. Questi prevedono la possibilità di allocare l'onere risarcitorio in base alla responsabilità effettiva di ogni titolare; nonché il diritto, per il titolare che abbia estinto l'intera obbligazione risarcitoria, di pretendere dagli altri contitolari una quota equivalente alla loro responsabilità. Ne consegue che l'accordo esterno, o quello interno laddove il primo non disponga in merito, diventa cruciale per la distribuzione delle responsabilità e per la determinazione dell'importo che ogni contitolare deve risarcire. Infatti, in assenza di un accordo chiaro o, in alternativa, di circostanze da cui dedurre la ripartizione degli oneri, l'obbligazione risarcitoria va suddivisa equamente, alla luce dei principi generali del diritto civile (art. 1298 c.c.).

A seguito di tali considerazioni, sorge spontaneo chiedersi se i contitolari possano accordarsi affinché un certo obbligo sia rimesso ad uno di loro soltanto[308];

---

[306]Tali obblighi di informazione sono sanciti agli artt. 13 e 14 del GDPR. Questi individuano, rispettivamente, le informazioni che il titolare deve fornire all'interessato quando: i dati personali vengono raccolti presso di lui (art. 13 GDPR); i dati personali non sono acquisiti dall'interessato (art. 14 GDPR).

[307]Per approfondimenti sull' accordo interno fra contitolari del trattamento, v. V. Colcelli, *Joint controller agreement under GDPR*, in *EU and Comparative Law Issues and Challenges Series*, 2019, n. 3, pp. 1038 e ss.

[308]Sull'obbligazione solidale e la sua ripartizione fra i condebitori, v. M. Bianca, *Diritto Civile. L'obbligazione*, Milano, Giuffrè, 2019, pp. 709 e ss., il quale precisa che non è l'obbligazione ad

in questo modo, il titolare onerato sarebbe l'unico a poter rispondere di un suo eventuale inadempimento. Da un simile scenario, deriverebbe un ulteriore conseguenza, ovvero che gli altri contitolari, una volta risarcito l'interessato, potrebbero rivalersi sul contitolare designato per l'intero importo versato; ciò, purché essi dimostrino che l'inadempimento era imputabile unicamente al titolare onerato. L'ipotesi prospettata evidenzia una problematica: spesso i contitolari devono collaborare per adempiere all'obbligazione; eppure, l'inadempimento non sempre è riconducibile a tutti loro, poiché potrebbe derivare dall'azione, o omissione, di un solo contitolare. In questo caso, il contitolare non inadempiente dovrebbe poter provare che la causa del danno è imputabile, in via esclusiva, all'altro contitolare. Così facendo, egli rimarrebbe solidalmente responsabile verso l'esterno, ma limiterebbe la propria responsabilità interna. Invero, il titolare (non inadempiente) potrebbe pretendere nei confronti del titolare (inadempiente) l'intero importo corrisposto a titolo risarcitorio, non solo la quota che spetterebbe all'inadempiente. A tal fine, però, il primo dovrebbe dimostrare che il danno è riconducibile esclusivamente alle azioni del contitolare onerato[309].

In conclusione, a prescindere dall'ultima questione sollevata, non può non evidenziarsi come entrambi gli accordi tra i contitolari assumano rilevanza in tema di responsabilità. L'accordo esterno, dando origine al rapporto di contitolarità, a seguito del quale <<è chiaro che sorge anche la responsabilità solidale di tutti>>[310]. L'accordo interno, rivestendo un ruolo fondamentale nella ripartizione della responsabilità fra i contitolari.

4.2. I soggetti esonerati dal regime di responsabilità solidale

Il sub-responsabile del trattamento

Diversamente dal contitolare, l'art. 82, par. 4, GDPR non estende il regime di responsabilità solidale al sub-responsabile del trattamento.

---

essere ripartita fra i condebitori, bensì la prestazione. Se, infatti, ad essere suddiviso fosse il credito verso i debitori o, viceversa, il debito verso i creditori, si tratterebbe di un'obbligazione parziaria, non solidale.

[309]A tal riguardo, è opportuno richiamare le riflessioni di A. D'Adda, *La solidarietà risarcitoria nel diritto privato europeo e l'art. 2055 c.c. italiano: riflessioni critiche*, in *Rivista di Diritto Civile*, 2016, n. 2, p. 303 e ss., il quale sottolinea che sono poche le occasioni in cui l'inadempimento di un condebitore è altresì riconducibile ad un altro dei soggetti obbligati; ciò, si riscontra solo quando la prestazione non eseguita sia strettamente correlata ad un'obbligazione altrui.

[310]F. Pizzetti, L. Greco, *Commento all'art. 26 Reg. 679/2016,* cit., p. 428.

Quanto a tale figura, si è già anticipato che la relazione tra questo e il *processor* costituiva una lacuna nella Direttiva 95/46 CE, mancando specifiche disposizioni in proposito. Successivamente, però, la Direttiva ePrivacy ha chiarito che, quando il fornitore di un servizio di comunicazione elettronica subappalta il trattamento dei dati personali, il subappalto e il trattamento devono essere pienamente conformi ai requisiti applicabili ai *processor* e *controller,* ai sensi dell'allora Direttiva 95/46 CE[311]. Tale affermazione implicava che il sub-trattamento dei dati, e i soggetti in esso coinvolti, rientrassero nell'ambito di applicazione della Direttiva 95/46 CE.

In merito alla responsabilità per il trattamento illecito dei dati, la Direttiva 95/46 CE individuava come unico responsabile il titolare del trattamento (art. 6); pertanto, questi era chiamato a rispondere anche per l'inadempimento del sub-responsabile. Essendo tale disposizione particolarmente gravosa per il *controller*, il Gruppo di lavoro "Articolo 29" suggeriva che, in caso di violazioni, il titolare potesse disporre di garanzie contrattuali contro il sub-responsabile e/o il responsabile. In dettaglio, l'accordo tra titolare e responsabile doveva prevedere che fosse il responsabile a rispondere, nei confronti del titolare, per le azioni del sub-responsabile; oppure, l'accordo fra responsabile e sub-responsabile doveva riconoscere un diritto del terzo a vantaggio del titolare. Quest'ultima soluzione era prospettabile in quanto l'accordo doveva essere concluso per conto del titolare, il quale diveniva parte contraente[312].

Al contrario, la Commissione Europea, riguardo al trasferimento di dati personali a responsabili del trattamento situati in Paesi terzi, precisava che era il *processor* a dover rispondere per l'inadempimento del *sub-processor.* Tuttavia, la Commissione aggiungeva che i sub-responsabili potevano altresì rispondere del danno nei confronti degli interessati qualora non fosse stato possibile avanzare una pretesa risarcitoria contro il titolare o il responsabile del trattamento. In questi casi,

[311]Il subappalto per il trattamento dei dati personali è disciplinato dal considerando n. 32 della Direttiva 2002/58 CE (Direttiva ePrivacy).
[312]In questo senso, v. Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 05/2012 sul* cloud computing *(WP 196*), 1 luglio 2012, par. 3.3.2, disponibile *online* su https://www.privacy.it/archivio/grupripareri201205.html#:~:text=Nel%20suo%20parere%2C%20il%20Gruppo,cloud%20con%20clienti%20nel%20SEE.

i *sub-processor* erano responsabili solo per le loro specifiche attività di trattamento[313].

Ebbene, la posizione assunta dalla Commissione non si discosta molto dalla soluzione adottata dal legislatore europeo. Il Regolamento, del resto, non si limita a disciplinare la figura del sub-responsabile, stabilendo che questa sia selezionata secondo i medesimi criteri usati dal titolare per la scelta del responsabile (art. 28, par. 4, GDPR), e che l'accordo tra responsabile e sub-responsabile soddisfi gli stessi obblighi di protezione dei dati previsti dall'accordo tra il titolare e il responsabile (art. 28, parr. 3 e 4, GDPR). All'opposto, il GDPR introduce un importante cambiamento in materia di responsabilità, in quanto statuisce che il *processor* è responsabile delle azioni del *sub-processor*. In questo modo, il Regolamento obbliga il primo ad assicurarsi che il secondo rispetti la legge sulla *data protection*, nonché a esercitare i poteri di controllo nei suoi confronti con maggiore attenzione[314].

Alla luce del Regolamento, quindi, il sub-responsabile è totalmente esonerato dal regime di responsabilità solidale. Il GDPR non contempla neppure l'ipotesi residuale di cui alla Decisione della Commissione, ossia che il sub-responsabile risarcisce il danno da provocato all'interessato <<qualora sia l'esportatore [titolare del trattamento] che l'importatore [responsabile del trattamento] siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi>>[315].

Il *Data Protection Officer*

Tra i soggetti solidalmente responsabili, l'art. 82, par. 4, GDPR non contempla neppure il *Data Protection Officer* (DPO), o responsabile della protezione dei dati. Tale figura rappresenta una novità rispetto alla previgente Direttiva, la quale non vi faceva alcun riferimento. Eppure, il DPO non era del tutto

---

[313]Sul punto, cfr. la Decisione 2010/87/UE della Commissione Europea del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi a norma della Direttiva 95/46 CE. In particolare, sulla responsabilità del sub-responsabile, v. artt. 18 e 20.

[314]Per un confronto sulla regolazione del *sub-processor* e della sua responsabilità nella Direttiva 95/46 CE, nella Decisione della Commissione e nel Regolamento, v. H.F. Küchler, *The Relations of Controllers, Processors and Sub-processors under the DPD and GDPR First Deliberations: Does the GDPR represent progress in the digital age?,* dicembre 2016, pp. 36 e ss., disponibile *online* su https://www.duo.uio.no/bitstream/handle/10852/54570/ICTLTHESIS_8016.pdf.

[315]Ai sensi dell'art. 20 della Decisione n. 2010/87/UE della Commissione Europea.

estraneo all'ordinamento europeo, giacché il Regolamento n. 45/2001 disciplinava già il responsabile per la protezione dei dati[316]. Il DPO non era sconosciuto neppure agli ordinamenti nazionali, quali l'Austria, la Repubblica Ceca e la Germania. Quest'ultimo fu il primo Paese ad introdurre, tramite il "*Bundesdatenschutzgesetz*", un precursore di tale ruolo: il "*datenschutzbeauftragter",* il quale presentava diversi aspetti in comune con il DPO del Regolamento[317].

Benché esistessero degli esempi di DPO, una regolazione puntuale dello stesso si è avuta solo con il GDPR. Secondo il Regolamento, non tutte le organizzazioni sono obbligate a nominare un DPO, ma vi sono tre ipotesi in cui un titolare o un responsabile del trattamento è tenuto a designarlo. Nello specifico, l'art. 37 GDPR impone la nomina del DPO allorchè il titolare sia un'istituzione pubblica, oppure quando il titolare e/o responsabile eserciti un'attività che comporti: un monitoraggio dei *data subject* ad ampio raggio; il trattamento massivo di dati appartenenti a categorie particolari, o relativi condanne e reati penali[318].

Passando ai compiti del DPO, occorre rilevare come il Regolamento, all'art. 39, ne fornisca un elenco apparentemente tassativo. La dottrina prevalente, però, ritiene che le funzioni previste dal GDPR vadano intese come requisiti minimi; dunque, non è escluso che il DPO possa svolgere altre attività, purché volte a proteggere i dati personali[319].

In base al Regolamento, il primo compito del DPO è informare *controller* e *processor* degli obblighi a cui sono sottoposti dal GDPR e dalle altre disposizioni comunitarie in materia di *data protection* (art. 39, par. 1, lett. a, GDPR). In secondo luogo, il legislatore europeo affida al DPO l'incarico di verificare la conformità al

---

[316]L'art. 24 del Regolamento 45/2001, rubricato <<responsabile della protezione dei dati>>, stabiliva che tutte le istituzioni europee nominassero almeno un responsabile della protezione dei dati, il quale, tra gli atri compiti, doveva assicurarsi che i trattamenti dei dati non ledessero i diritti dei *data subject.*

[317]Pur esistendo diversi punti di contatto tra il DPO e il *datenschutzbeauftragte*r, sussistono anche delle notevoli differenze. Ad esempio, per la figura tedesca, l'obbligo di nomina riguarda solo gli enti che abbiano un certo numero di dipendenti addetti alla gestione dei dati personali. Per un'analisi approfondita sul *datenschutzbeauftragter,* v. K. A. Bamberger, D. K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, in *George Washington Law Review*, 2013, n. 81, pp. 1574 e ss.

[318]Sulla nomina obbligatoria del DPO, v. F. Ciclosi, F. Massacci, *The Data Protection Officer, a ubiquitous role nobody really knows*, in *IEEE Security and Privacy,* vol. XXI, 2022, n. 1, pp. 66 e ss.

[319]Tra tutti, v. G. Bellomo, *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO*), marzo 2020*,* pp. 11 e ss., disponibile *online* su https://ricerca.unich.it/retrieve/e4233f17-76f2-2860-e053-6605fe0a460a/bellomo_scrittiCostanzo.pdf.

Regolamento, alla disciplina sulla *data protection*, come pure alle politiche del titolare o del responsabile relative alla protezione dei dati personali (art. 39, par. 1, lett. b, GDPR). Qualora gli sia richiesto, il DPO è altresì tenuto a fornire consulenza riguardo alla valutazione d'impatto sulla protezione dei dati e a monitorarne l'esecuzione ai sensi dell'art. 35 GDPR (art. 39, par. 1, lett. c, GDPR). In quarto luogo, il DPO è chiamato a collaborare con l'autorità di controllo, la quale deve poter contare su tale figura per ogni problematica relativa al trattamento, compresa la consultazione preventiva di cui all'art. 36 GDPR. (art. 39, par, 1, lett. d ed e, GDPR). Infine, il DPO può fornire chiarimenti agli interessati sulle fasi del trattamento che coinvolgano i loro dati, nonché sui diritti che spettano loro in virtù del GDPR (art. 38, par. 4, GDPR)[320].

Malgrado il *Data Protection Officer* svolga funzioni di rilievo per la gestione dei dati, egli non può essere ritenuto responsabile per un trattamento che si discosti dal Regolamento; di una simile inosservanza, dovranno rispondere il titolare, o il responsabile. Questi, d'altronde, sono gli unici ad essere gravati da un onere di conformità al Regolamento ai sensi degli artt. 82 e 83 GDPR[321].

Sebbene i danni da mancata *compliance* non siano direttamente imputabili al DPO, è comunque vero che, qualora tali inosservanze derivino dal dolo o dalla colpa grave di quest'ultimo, il titolare e il responsabile possono agire in regresso nei suoi confronti. Pertanto, il DPO non è tenuto a rispondere in solido con gli altri attori del trattamento, ma il suo inadempimento può dar luogo a <<pretese risarcitorie interne>>[322].

[320]Circa il ruolo del DPO, v. R. Szalowski*, Data Protection Officer in the light of the provisions of the General Data Protection Regulation (GDPR*), in *Ius Novum*, 2018, n.4, pp. 120 e ss.
[321]In questi termini, Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01),* 13 dicembre 2016, par. 12, disponibile *online* su https://ec.europa.eu/newsroom/article29/items/612048.
[322]A. Avitabile, *Il* Data Protection Officer, in G. Finocchiaro (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* cit., p. 355.

Capitolo III

Il *Data Processing Agreement*: uno strumento chiave per la ripartizione delle responsabilità

Sommario: 1. Il *Data Processing Agreement;* 1.1. Il contratto di *outsourcing*: natura giuridica e diffusione; 1.2. Il contratto di *outsourcing* nel trattamento dei dati. La suddivisione dei ruoli; 1.3. La designazione del *processor* prima e dopo il GDPR; 2. *Internet of Things,* un ambito complesso in cui il DPA assume una funzione cruciale; 2.1. La diffusione dei sistemi IoT nella società odierna; 2.1.1. Le *Smart Homes*: un esempio emblematico dell'importanza del *Data Processing Agreement*; 2.2. Profili critici della negoziazione nell'universo IoT, e non solo; 2.2.1. Conformità del *Data Processing Agreement* al GDPR. La posizione dell'autorità svedese nel caso del Comune di Salem; 2.3. Il *Cloud of Things*: una pluralità di contratti e di contraenti; 3. Il *Cloud Computing* e la distribuzione dei ruoli alla luce del GDPR; 3.1. *Cloud Consumer* e *Cloud Service Provider*, titolari o responsabili del trattamento?; 3.1.1. Il caso *Wirtschaftsakademie;* 3.1.2. Dal caso *Wirtschaftsakademie* al caso *Fashion ID*: una lettura più restrittiva della contitolarità; 3.2. La contitolarità nei termini di servizio dei *cloud service provider;* 3.3. La struttura dei contratti di *cloud computing;* 3.3.1. Il *Data Processing Agreement* e il difficile adattamento al modello del *cloud computing;* 4. Responsabilità e allocazione dei costi nel *Data Processing Agreement*

1. Il *Data Processing Agreement*

Il GDPR ha profondamente modificato l'impianto regolatorio europeo in materia di trattamento dei dati personali. Tale cambiamento emerge, in particolar modo, dalla comparazione tra il testo della previgente Direttiva e l'art. 28 del GDPR. Quest'ultimo, infatti, non si limita a prevedere che <<l'esecuzione dei trattamenti su commissione [sia] disciplinata da un contratto o da un atto giuridico>>[323]; al contrario, richiede che l'atto con cui il titolare affidi il trattamento al responsabile (*Data Processing Agreement* o DPA) soddisfi specifici oneri formali e sostanziali.

[323] Ai sensi dell'art. 17, par. 3, della previgente Direttiva 95/46 CE.

Un approccio così diverso dal precedente ha alla base una pluralità di motivazioni. Prima tra tutte, l'affermazione del principio di *accountability*, dal momento che il legislatore, in un'ottica di responsabilizzazione degli attori del trattamento, ha imposto obblighi tanto al *controller,* quanto al *processor.* Ciò ha reso fondamentale che questi fossero ripartiti all'interno di un atto giuridicamente vincolante, quale il DPA. A questo motivo, se ne aggiunge un altro ancor più evidente, ovvero lo stesso che ha indotto il legislatore ad adottare un Regolamento, piuttosto che una Direttiva: l'esigenza di garantire un trattamento dei dati uniforme tra gli Stati Membri[324]. D'altronde, il cambiamento in esame appare altresì riconducibile al contesto economico in cui il Regolamento è stato adottato. In quegli anni, il mercato è stato "scosso" da una vera e propria rivoluzione digitale, nonché da un processo che ha riguardato le principali aziende europee, le quali tendevano ad esternalizzare parte delle loro attività presso altre imprese, realizzando il cosiddetto *outsourcing.* In un simile scenario, caratterizzato dal rafforzamento dei fornitori di servizi, e dall'indebolimento dei loro utilizzatori, la previsione di un contenuto obbligatorio per il DPA ha rappresentato il tentativo di riportare un equilibrio tra le parti[325].

1.1. Il contratto di *outsourcing*: natura giuridica e diffusione

Soffermandoci meglio sul concetto di "*outsourcing*", si osserva come tale espressione sia adoperata per riferirsi ad un'azienda (*outsourcer*) che si rivolge ad un soggetto esterno (*outsourcee*) affinché questi esegua attività di norma gestite internamente (la cd. esternalizzazione)[326]. Solitamente, l'*outsourcer* adotta questa strategia quando intende concentrarsi sulla propria attività principale, affidando le operazioni secondarie a un terzo. Del resto, una simile redistribuzione delle funzioni

[324]In questi termini S. Calzolaio et al., *La responsabilità e la sicurezza del trattamento*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/67,* Napoli, Editoriale scientifica, 2017, pp. 154 e ss.

[325]Così A. Chiappini, *Riflessioni sul contratto tra titolare e responsabile del trattamento*, in *Contratto e Impresa*, 2021, n. 1, pp. 317 e ss.

[326]Per una definizione di esternalizzazione, v. Cass. 17 aprile 2012, n. 5997, in *Argomenti di Diritto del Lavoro*, 2012, 4, 974, con nota di A. Riccobono, *Verso una tipizzazione del "contratto di esternalizzazione"*?, secondo cui <<l'espressione ricomprende in senso lato ogni ipotesi di decentramento produttivo che determina un mutamento di titolarità attiva dei rapporti di lavoro>>.

permette all'azienda di convogliare le proprie risorse, umane e finanziarie, sul cuore della produzione, traendone un indubbio beneficio economico[327].

L'esigenza di non disperdere le risorse interne è diventata tanto più impellente con l'avanzare del progresso tecnologico. Per "stare al passo", le imprese si sono viste costrette ad investire tempo e denaro nei processi di ammodernamento, a scapito della loro produttività. In un contesto simile, non sorprende che abbiano assunto un ruolo cardine le aziende specializzate nella "Tecnologia dell'Informazione" (IT), ossia quelle che si servono di sistemi informatici, quali *hardware* e s*oftware*, per sviluppare informazioni. Nello specifico, tali imprese offrono servizi informatici ad altre compagnie, permettendo loro di dedicarsi al proprio *core business*[328]. Come per le altre ipotesi di esternalizzazione, quindi, anche nell'ambito IT gli accordi di *outsourcing* hanno ad oggetto la prestazione continuativa di servizi, in questo caso di natura informatica. I contratti di IT *outsourcing*, però, non comportano vantaggi solo per l'azienda esternalizzatrice, che può accedere a competenze tecnologiche avanzate, razionalizzare i costi di produzione e impiegare al meglio le risorse interne, ma anche per il mercato. Difatti, la combinazione di nuove tecnologie a disposizione e abbattimento dei costi consente all'impresa di competere in modo più efficace, favorendo l'instaurazione di assetti concorrenziali[329].

Nell'ambito dell'IT *outsourcing*, inteso in senso ampio, si colloca anche un particolare tipo di erogazione di servizi informatici nota come "*cloud computing*", che consente l'accesso a risorse tecnologiche tramite connessione online. Ciò che distingue tale sistema rispetto ad altri è la possibilità, per gli utenti, di usufruire delle risorse attraverso i *server* forniti da soggetti terzi, senza acquisirne la proprietà[330]. Tuttavia, non esiste un'unica tipologia di *cloud computing*, essendo

---

[327]Sui vantaggi dell'*outsourcing*, v. M. Pittalis, Outsourcing, in *Contratto e Impresa*, 2000, n. 2, pp. 1006 e ss., la quale, fra gli altri, menziona la riduzione dei costi operativi, data dall'aumento di incidenza dei costi variabili e dalla riduzione di quelli fissi; nonché, la disponibilità di strumenti tecnologicamente più avanzati rispetto a quelli posseduti dall'azienda; ed infine, la diminuzione dei rischi legati alla gestione dell'attività esternalizzata.

[328]Per un approfondimento sui contratti di *outsourcing* conclusi nel settore IT, v. F. Tosi, *Il contratto di* outsourcing *di sistema informatico*, Milano, Giuffrè, 2001, pp. 5 e ss., che rileva come la ragione per cui le aziende siano ricorse al contratto di *outsourcing* di servizi informatici sia variato nel tempo: inizialmente, le aziende non godevano degli strumenti adeguati; in un secondo momento, queste si rivolgevano a fornitori esterni solo per le operazioni più complesse; da ultimo, si è sviluppato il vero e proprio <<*out*>>, termine con cui l'autore si riferisce all'*outsourcing.*

[329]Sugli effetti positivi degli accordi di IT *outsourcing,* v. M. Beretta, C. Rizza, *Divieto di concentrazione e accordi di IT* outsourcing, in *Il Diritto Industriale*, 2004, n. 3, pp. 245 e ss.

[330]A tal proposito, v. A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di* cloud computing, in *Contratto e Impresa*, 2012, nn. 4-5, pp. 1216 e ss.

state individuate tre categorie distinte a seconda del servizio offerto all'utilizzatore: l'accesso ad un *software*, nel caso del *cloud software as a service*; la disponibilità di un'intera piattaforma, nel caso del *cloud platform as a service*; l'utilizzabilità di un *hardware,* nel caso del *cloud infrastructure as a service*. In ognuna di queste ipotesi, il servizio è gestito da un terzo, impresa IT, in modalità remota[331].

In virtù di quest'ultima caratteristica, si è soliti far rientrare il *cloud computing* nel fenomeno dell'*outsourcing*. Eppure, i modelli contrattuali adottati per le due fattispecie non sono perfettamente identici. Per quanto riguarda il contenuto, ad esempio, sebbene entrambi stabiliscano gli standard per la valutazione delle *performance*, e definiscano i criteri sulla base dei quali apprezzare l'efficienza della prestazione, si differenziano sotto altri profili. Tra tutti, riveste particolare importanza quello relativo al tipo di risorse oggetto dell'esternalizzazione, che deve essere espressamente definito dalle parti. Mentre l'*outsourcer* è solito esternalizzare tanto le risorse edilizie, strumentali e organizzative, quanto quelle di personale, al fine di integrare la propria forza lavoro con quella dell'*outsourcee*; nel *cloud computing* non si avverte un simile bisogno di manodopera esterna, perché il servizio si fonda principalmente su componenti organizzative e strutturali[332].

Inoltre, i modelli differiscono per la struttura contrattuale adoperata, che non può non adattarsi alle modalità di erogazione del servizio. Nel *cloud computing*, esso è rivolto a una pluralità di clienti e tende, pertanto, ad essere tipizzato. Diversamente, nell'*outsourcing,* il servizio è generalmente indirizzato ad un singolo, o comunque ad un numero limitato di beneficiari, perciò è maggiormente caratterizzato. Quanto agli effetti di una simile diversificazione, questi sono riscontrabili già durante la fase di negoziazione, la cui durata è maggiore o minore a seconda del livello di personalizzazione richiesto per il servizio e, di conseguenza, per le clausole contrattuali. In genere, le suddette clausole sono standard negli accordi di *cloud computing*, ove gli utenti possono accettare le condizioni prospettategli, oppure rinunciarvi e rivolgersi ad un altro fornitore[333]. All'opposto,

---

[331]Circa la classificazione dei servizi *cloud,* v. A. Ricci, *L'*outsourcing *e* cloud computing, in F. Delfini, G. Finocchiaro (a cura di), *Diritto dell'informatica*, Torino, UTET, 2014, pp. 672 e ss.

[332]Sulle somiglianze e le differenze dei due modelli contrattuali, v. A. Mantelero, *Il contratto per l'erogazione alle imprese di servizi di* cloud computing, cit., pp. 1217 e ss.

[333]Per un'analisi accurata sui contratti di *cloud computing*, v. S. Bradshaw, C. Millard, I. Walden, *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, in *International Journal of Law and Information Technology*, vol. IXX, 2011, n. 3, pp. 196

nei contratti di *outsourcing,* le clausole vengono definite dalle parti, le quali hanno interesse a concludere accordi duraturi. Per tale motivo, esse prevedono anche la rinegoziabilità di alcune condizioni, cosicché i contratti possano conformarsi alle esigenze future.

L'ampia libertà negoziale delle parti è strettamente correlata alla natura dell'*outsourcing*, il quale, essendo privo di una regolamentazione puntuale, configura una fattispecie atipica per il nostro ordinamento. In virtù di ciò, gran parte della dottrina ha ritenuto che questa debba essere sussunta sotto diverse categorie contrattuali esistenti (ad es. la locazione, l'appalto, la somministrazione ecc.). Difatti, secondo questo orientamento, qualora alcuni aspetti del rapporto non siano definibili dai contraenti, deve trovare applicazione il criterio dell'analogia, che impone di ricorrere alla disciplina del modello legale più simile[334]. Alla luce di tale criterio, occorre comprendere a quale tipo di contratto possa essere ricondotto l'*outsourcing* informatico. A questo proposito, la dottrina ha rilevato che, seppur in ambito IT l'*outsourcing* sia utilizzato per rispondere a esigenze tra di loro eterogenee, esso si sostanzia sempre in una fornitura di servizi da un soggetto ad un altro. In questa prospettiva, l'*outosurcing* non può che essere inquadrato nel contratto tramite cui <<una parte assume, con organizzazione dei mezzi necessari e con gestione a proprio rischio, il compimento […] di un servizio verso un corrispettivo in danaro>>[335]: l'appalto di servizi. D'altronde, ripercorrendo le norme del codice civile, questa appare l'unica conclusione accettabile. Invero, l'*outsourcing* non può essere ricondotto al contratto di prestazione d'opera, in cui il prestatore si impegna a svolgere personalmente il lavoro in favore del committente. Al contrario, l'accordo di *outsourcing* presuppone che l*'outsourcee* disponga di un'adeguata organizzazione di risorse umane e strutturali, avendo assunto la gestione di un intero servizio dell'*outsourcer*[336].

Tantomeno il contratto di *outsourcing* ricade nell'ipotesi della locazione, che pure si rinviene nella fattispecie in esame. Del resto, l'*outsourcee* gode dei beni

---

e ss., i quali prendono in considerazioni alcune fra le clausole più ricorrenti, come quelle in materia di legge applicabile, giurisdizione, arbitrato, integrità e conservazione dei dati.

[334]Tra tutti, v. F. Cardarelli, *La cooperazione fra le imprese nella gestione di risorse informatiche: aspetti giuridici del c.d*. <<outsourcing>>, in *Diritto dell'informazione e dell'informatica,* 1993, n.1, pp. 94 e ss.

[335]Ai sensi dell'art. 1655 c.c.

[336]Con riguardo alle discrepanze tra i due contratti, cfr. D. Rubino, G. Iudica, *Appalto*, in F. Galgano (a cura di), *Commentario al codice civile Scialoja – Branca*, Bologna, Zanichelli, pp. 26 e ss.

che compongono il sistema dell'*outsourcer* solo per adempiere alla sua obbligazione principale, ossia amministrare tale sistema. Di conseguenza, la locazione, in base al principio dell'assorbimento[337], non incide sulla qualificazione giuridica del contratto di *outsourcing.* Per il medesimo principio, l'*outsourcing* non può essere inscritto neppure nel contratto di somministrazione, considerato che la prestazione di dare si colloca in posizione secondaria rispetto a quella di fare[338]. Talvolta, però, la disciplina della somministrazione può essere applicata anche alle ipotesi di *outsourcing*. La ragione di ciò risiede nell'art. 1677 c.c., il quale estende, <<in quanto compatibili>>, le norme della somministrazione all'appalto di servizi[339]. Dunque, esse sono applicabili solo laddove il contratto di o*utsourcing* sia concepito come appalto di servizi. Come anticipato, questa qualificazione sembra essere la più convincente, in quanto l*'outsourcing* presenta tutti gli elementi tipici dell'appalto, quali: l'adempimento di una prestazione in cambio di un corrispettivo, l'organizzazione autonoma delle risorse necessarie, nonché l'assunzione del rischio di impresa, comprensivo di eventuali perdite o danni[340].

1.2. Il contratto di *outsourcing* nel trattamento dei dati. La suddivisione dei ruoli

Com'è stato appena evidenziato, le imprese tendono ad attribuire a terzi la cura di attività accessorie rispetto a quella principale. Tali attività, però, spesso comportano il trattamento di dati da parte della persona fisica o giuridica a cui sono state affidate, ragion per cui l'azienda esternalizzatrice ricorre al contratto di *outsourcing* anche per disciplinare il *data processing*[341].

---

[337] Secondo il criterio dell'assorbimento, il contratto misto deve essere regolato seguendo la disciplina del tipo legale in esso "prevalente". Per individuarlo, occorre tener conto del profilo funzionale. Sul punto, cfr. Cass. sez. un. 12 maggio 2008, n. 11656, in *Immobili & proprietà*, 2008, n. 9, con nota di R. Triola, *Cosa Futura*.

[338]Sull'applicazione della teoria dell'assorbimento, o prevalenza, al contratto di *outsourcing,* v. A. Musella, *Il contratto di* outsourcing *del sistema informativo*, in *Diritto dell'informazione e dell'informatica,* 1998, n. 1, pp. 859 e ss.

[339]Per valutare se la normativa sia applicabile o meno al caso concreto, uno dei fattori da considerare è l'*intuitus personae*: tanto più forte è il vincolo fiduciario alla base dell'accordo, tanto più circoscritta è l'operatività della disciplina che regola la somministrazione. In questo senso, v. Coll. Arb., 11 novembre 1985*,* in *Nuova Giurisprudenza Civile Commentata*, 1986, n. 1, con nota di A. Ballestreri.

[340]Sugli elementi costitutivi della fattispecie di appalto, v. nota 13.

[341]Per un'attenta disamina sul contratto di *outsourcing* in ambito di *data protection*, v. L. Greco. *I ruoli: titolare e responsabile*, cit., pp. 274 e ss.

Eppure, il fatto che esistano due entità separate non permette di individuare la funzione che esse assumono nel trattamento dei dati, poiché non implica necessariamente che entrambe abbiano autonomia nella gestione dei dati e, quindi, che siano dei *controller.* Parimenti, il rapporto economico che caratterizza le parti, ovvero chi ha esternalizzato il servizio e chi lo ha preso in carico, non costituisce un indice del ruolo che rivestono nel trattamento. In definitiva, il solo criterio utilizzabile, così come per le altre ipotesi di *data processing*, rimane quello funzionale, che impone di verificare se la scelta dei mezzi e delle finalità del trattamento sia esclusivo appannaggio dell'*outsourcer*. Se così fosse, questo sarebbe l'unico titolare, mentre l'*outsourcee* assumerebbe la veste di responsabile. In caso contrario, vale a dire se ciascuno dei soggetti avesse potere decisionale sugli elementi che contraddistinguono il trattamento (strumenti e scopo), sussisterebbero due diversi *controller*[342].

D'altronde, l'esistenza di due titolari, piuttosto che un titolare e un responsabile, ha delle notevoli ricadute sul piano organizzativo, nonché su quello della responsabilità. Qualora sia l'*outsourcer* che l'*outsourcee* ricoprissero la funzione di *controller,* il primo sarebbe sollevato dagli obblighi inerenti la fase di trattamento di competenza del secondo. Di conseguenza, l'*outsourcer* sarebbe esonerato dalla responsabilità per gli illeciti commessi dall'*outsourcee* nell'adempimento di tali oneri. Tuttavia, colui che avesse esternalizzato il trattamento potrebbe dover rispondere dei danni indiretti, come quello alla reputazione. Per tutelarsi da questa eventualità, l'*outsourcer* potrebbe decidere di inserire nel DPA delle clausole che stabiliscano *ex ante* l'ammontare dei danni risarcibili, oppure che prevedano la risoluzione dell'accordo allorchè l'*outsourcee*, disponendo dei dati dell'*outsourcer*, cagioni un pregiudizio a qualcuno[343]. La responsabilità non è l'unico aspetto ad essere influenzato dalla modalità di

---

[342]A sostegno dell'imprescindibilità del criterio funzionale, v. A. Mantelero, *Processi di* outsourcing *informatico e* cloud computing*: la gestione dei dati personali ed aziendali*, in *Diritto dell'informazione e dell'informatica,* 2010, nn. 4-5, pp. 680 e ss., il quale richiama le osservazioni precedentemente esaminate del Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento",* cit*.,* sull'inapplicabilità del criterio formale, a favore di quello funzionale.

[343]Per una riflessione generale sull'importanza della rinegoziazione nei contratti di *IT outourcing*, v. T. Baratta, *Le sopravvenienze e la clausola di rinegoziazione nei contratti di* outsourcing d*i sistema informatico tra buona fede e autonomia privata*, in P. Perlingieri (a cura di), *Rassegna di diritto civile*, vol. III, Napoli, Edizioni Scientifiche Italiane, 2018, pp. 800 e ss., la quale sottolinea che <<la clausola di adeguamento contrattuale consente tanto all'*outsourcer*, quanto all'impresa servita, […] di convocare la controparte a sedersi al tavolo delle trattative e rinegoziare determinati assetti negoziali>>.

organizzazione del trattamento, giacché questa incide anche sull'informativa destinata all'interessato. Infatti, il *controller,* prima di incaricare un terzo della gestione dei dati, deve comunicarlo al *data subject*, indicandogli le finalità del trattamento, nonché il soggetto designato ad effettuarlo (art. 13 GDPR).

Laddove il *data processing* fosse operato dall'*outsourcer,* in qualità di *controller,* e dall'*outsourcee,* in qualità di *processor*, questo avrebbe degli effetti diversi sulla distribuzione della responsabilità. In particolare, il *processor* risponderebbe del danno solo al verificarsi delle condizioni di cui all'art. 82, par. 2, GDPR (inosservanza delle istruzioni del titolare e degli obblighi specificatamente rivoltigli dal Regolamento); o solidalmente al *controller*, se entrambi fossero responsabili per il pregiudizio derivante dal trattamento (art. 82, par. 4, GDPR).Quanto all'obbligo di informare l'interessato, invece, non sussisterebbero differenze, poiché questi ha il diritto di sapere quando i propri dati vengono affidati ad un responsabile del trattamento, così come ad un altro titolare[344].

1.3. La designazione del *processor* prima e dopo il GDPR

Supponendo che il contratto di *outsourcing* sia adoperato per nominare un *processor*, questo deve essere stipulato in conformità al GDPR. Infatti, il Regolamento ha introdotto delle modifiche sia riguardo al contenuto dell'atto di designazione del responsabile, gravandolo di nuovo obblighi e responsabilità, che riguardo ai requisiti formali dello stesso.

Quanto a tale aspetto, la Direttiva prevedeva già un obbligo di forma scritta, ma questa aveva un valore meramente probatorio[345]. Con l'introduzione del GDPR, il legislatore europeo ha inasprito la condizione formale, imponendo alle parti un onere *ad substantiam:* qualora non venga utilizzata la forma scritta, la nomina del responsabile è da considerarsi nulla[346].

---

[344]Sul contenuto dell'informativa all'interessato, v. F. De Stefani, *Le regole della privacy. Guida pratica al nuovo GDPR*, cit., pp. 52 e ss. In particolare, cfr. tabella riepilogativa p. 61.

[345]L'art. 17, par. 4, della Direttiva 95/46 CE prevedeva la forma scritta << a fini di conservazione delle prove>>. In questo senso doveva essere letta anche la normativa nazionale, dal momento che il legislatore, all'art. 29 del d.lgs. 196/2003, non aveva indicato alcuna sanzione per l'inosservanza del requisito di forma. Sul punto, v. G. M. Riccio, *Soggetti che effettuano il trattamento*, in S. Sica, P. Stanzione (a cura di), *La nuova disciplina della privacy - d.lgs. 20 giugno 2003, n. 196,* Bologna, Zanichelli, 2004, pp. 123 e ss.

[346]Circa il vincolo di forma nel GDPR, v. D. Farace, *Il titolare e il responsabile del trattamento*, in V. Cuffaro et al. (a cura di), *I dati personali nel diritto europeo*, cit., pp. 762 e ss.

Passando al profilo sostanziale, si osserva come il GDPR, a differenza della Direttiva, abbia individuato degli elementi che devono necessariamente essere regolati all'interno del *Data Processing Agreement*. In primo luogo, il DPA deve stabilire l'oggetto e la durata del trattamento, come pure la natura e lo scopo dello stesso, la tipologia di dati e di interessati coinvolti, nonché i diritti ed oneri del *controller* (art. 28, par. 3, GDPR). In aggiunta a questa parte generale, il Regolamento descrive ulteriori clausole che devono essere incluse, le quali sono strettamente correlate agli obblighi del responsabile. Invero, l'accordo deve chiarire quali sono gli oneri del *processor* in materia di riservatezza (art. 28, par. 3, lett. b, GDPR) e sicurezza (art. 28, par. 3, lett. c). In relazione all'obbligo del titolare di scegliere un responsabile adeguato, il contratto deve altresì stabilire che il *processor* predisponga misure tali da consentire al *controller* di soddisfare le richieste del *data subject* circa l'esercizio dei propri diritti (art. 28, par. 3, lett. e, GDPR). Inoltre, il DPA deve imporre al *processor* di aiutare il titolare ad adempiere alle proprie responsabilità nel rispetto del Regolamento; nello specifico, a conformarsi agli obblighi di cui agli artt. 32 e 36 GDPR sulla sicurezza del trattamento e la consultazione con l'Autorità di controllo (art. 28, par. 3, lett. f, GDPR). Fra le varie clausole, l'accordo deve anche contenerne una che obblighi il *processor* a partecipare alle operazioni di audit avviate dal titolare, come pure a condividere con questo le informazioni idonee a dimostrare l'osservanza degli obblighi di cui all'art. 28 GDPR (art. 28, par. 3, lett. h, GDPR). Tale ultima previsione permette di ottemperare ad un altro dovere sancito dal GDPR, quale quello di conservazione della documentazione. Infine, il contratto deve prevedere che il responsabile elimini o restituisca i dati personali una volta terminata la prestazione (art. 28, par. 3, lett. g, GDPR). Benché ciò derivi dall'obbligo del *processor* di agire secondo le istruzioni del *controller,* il legislatore sottolinea l'importanza della cancellazione o restituzione dei dati, chiedendo alle parti di esplicitarla nel DPA.

2. *Internet of Things*, un ambito complesso in cui il DPA assume una funzione cruciale

Alla luce dell'art. 28 poc'anzi analizzato, emerge come il Regolamento disciplini in modo dettagliato il contratto tra titolare e responsabile del trattamento. Tuttavia, i rapporti tra le parti sono diventati piuttosto complicati a causa del rapido sviluppo tecnologico che sta interessando la società. Una velocità simile non era di

certo prevedibile dal legislatore europeo, ragion per cui il GDPR non sempre riflette il rapporto che, nella realtà, si viene a creare tra *processor* e *controller.* Del resto, la circostanza che gli attori del trattamento operano all'interno di un "universo digitale" non poteva non influire sulle loro dinamiche relazionali. In particolare, ciò risulta evidente se si pensa all' *Internet of Things*, o IoT. In tale contesto, non solo è frequente che più soggetti collaborino nella gestione dei dati, ma è altresì probabile che lo status di un fornitore di servizi IoT vari tra *controller* e *processor* a seconda delle circostanze[347]. Per questo motivo, può risultare difficile determinare chi sia responsabile per i danni derivanti dal trattamento. Dinanzi a questa incertezza, il DPA assume un ruolo fondamentale, poiché rappresenta lo strumento attraverso cui le parti possono ripartire chiaramente le rispettive responsabilità.

Prima di approfondire quanto finora accennato, occorre chiarire il concetto di "*Internet of Things*", con cui si è soliti riferirsi a:

> un'infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano ("oggetti" a sé stanti oppure oggetti connessi ad altri oggetti o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete[348].

L'espressione "*Internet of Things*", quindi, è stata introdotta per identificare il sistema di oggetti collegati in rete che consente la connettività in qualsiasi momento e in qualsiasi luogo. Nello specifico, le *smart things* utilizzano i sensori e gli attuatori[349] di cui sono dotate per raccogliere dati dalla realtà circostante e

---

[347]In questo senso, v. J. Lindqvist, *New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?,* in *International Journal of Law and Information Technology*, 2018, n. 26, pp. 46 e ss., la quale evidenzia come, in ambito IoT, sia necessario che le parti definiscano i loro ruoli durante il trattamento dei dati, poiché ciò si ripercuote inevitabilmente sulla ripartizione delle responsabilità.

[348]Gruppo di lavoro per la protezione dei dati personali (Art. 29), *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti* (WP 223), 16 settembre 2014, p. 4, disponibile *online* su https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf.

[349]Sensori e attuatori sono tra gli elementi costitutivi dell'IoT. In molte applicazioni IoT, l'impiego di uno o più sensori è indispensabile per raccogliere dati e informazioni sul sistema: i sensori di umidità forniscono dati per controllare i sistemi di irrigazione; i sensori di traffico forniscono dati per controllare i semafori; i sensori di occupazione forniscono dati per controllare gli ambienti degli edifici. Quanto agli attuatori, questi sono dispositivi capaci di determinare cambiamenti fisici nell'ambiente; si pensi, ad esempio, all'apertura di una valvola, o all'accensione di un motore. Per una disamina dei diversi tipi di sensori e attuatori che ricorrono in ambito IoT, v. A. Schmidt, K. Van Learhoven, *How to Build Smart Appliances*?, in *IEEE Personal Communications*, vol. VIII, 2021, n. 4, pp. 66 e ss.

trasmetterli ad altri "oggetti intelligenti", essendo a questi connessi tramite reti cablate e wireless[350].

2.1. La diffusione dei sistemi IoT nella società odierna

L'installazione di nuove reti wireless, insieme allo sviluppo di sensori all'avanguardia, ha favorito l'uso di applicazioni IoT in diversi settori.

Energia

Il consumo di energia a livello globale è in continuo aumento; pertanto, mai come adesso, si avverte l'esigenza di una soluzione energetica più "intelligente". In risposta a tale necessità, gli enti pubblici e privati si sono mossi verso una gestione efficiente dell'energia, che comprende sia soluzioni semplici come l'impiego di lampadine intelligenti, sia soluzioni più complesse, come rendere alcune piattaforme petrolifere *offshore* completamente autonome. In generale, l'IoT sta rivoluzionando molti settori dell'industria energetica, dalla produzione dell'energia alla sua trasmissione e distribuzione.

Per comprendere l'importanza degli applicativi IoT nel settore energetico, è sufficiente considerare come essi semplifichino il monitoraggio dei sistemi energetici, soprattutto l'efficienza delle prestazioni, e come ciò si ripercuota positivamente sulla loro manutenzione. Ancora, le soluzioni IoT possono essere utilizzate per migliorare la sicurezza operativa e prevenire gli incidenti di produzione. A tal proposito, occorre evidenziare che una delle principali aree di applicazione dell'*Internet of Things* è quella dei droni, i quali esercitano una funzione importante nella gestione del rischio, essendo adoperati per scongiurare incidenti nelle centrali nucleari o nei siti minerari[351].

Sanità

Gli effetti del fenomeno IoT sono altresì rilevabili nel settore sanitario, specialmente dopo la recente crisi pandemica che ha accelerato la diffusione di oggetti intelligenti. Difatti, si è registrata una crescita della domanda di dispositivi

[350]Per ulteriori precisazioni sul concetto di IoT, v. di S. Madakam, R. Ramaswamy, S. Tripath, *Internet of Things (IoT): A Literature Review*, in *Journal of Computer and Communications*, 2015, n. 3, pp. 165 e ss.
[351]Sui risvolti dell'IoT in ambito energetico, v. N. Hossein Motlagh et al., *Internet of Things (IoT) and the Energy Sector*, in *Energies*, 2020, n. 13, pp. 494 e ss.

sanitari IoT specifici, come quelli ideati per la telemedicina, la diagnostica digitale, il monitoraggio remoto e l'assistenza robotica. D'altra parte, questi strumenti apportano innumerevoli vantaggi al sistema sanitario, tra cui la riduzione dei tempi di attesa per l'assistenza ospedaliera, l'agevolazione nel tracciamento dei pazienti, nonché una gestione più rapida di attività pratiche, quale l'inventario dei farmaci[352].

Agricoltura

La popolazione mondiale è in aumento e, secondo recenti studi, si prevede che continuerà a crescere, raggiungendo gli 8,6 miliardi nel 2030, i 10 miliardi nel 2050 e gli 11,2 miliardi nel 2100[353]. Ebbene, un simile sviluppo demografico implica la necessità di un altrettanto significativo incremento di risorse alimentari, che possono essere assicurate solo coniugando l'agricoltura con le nuove tecnologie. Tutto ciò spiega l'importanza assunta dall'IoT, che offre soluzioni prima impensabili, come la serra "intelligente". Quest'ultima ha rivoluzionato l'agricoltura, poiché, grazie a sensori, motori e sistemi di monitoraggio che migliorano le condizioni ambientali e automatizzano il processo di crescita delle piante, consente di creare un microclima autoregolato, ideale per il ciclo vitale delle colture[354].

Edilizia

Tra le aree maggiormente influenzate dall'IoT, spicca sicuramente quella dell'edilizia. D'altronde, una delle principali innovazioni introdotte dall'*Internet of Things* sono le cosiddette "*smart homes",* o case intelligenti. Con tale espressione si intendono edifici che integrano dispositivi di rilevamento e controllo, quali luci automatizzate, serrature elettroniche e molti altri ancora, collegati gli uni agli altri tramite connessione wireless. Grazie alla connettività di rete, coloro che risiedono

---

[352]Per approfondimenti sull'utilizzo degli applicativi IoT nel sistema sanitario, v. la relazione tenuta da F. Hu, D. Xie, S. Shen alla "*IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*" del 2013, dal titolo "*On the Application of the Internet of Things in the Field of Medical and Health Care"*, pp. 2053 e ss, disponibile *online* su https://www.computer.org/csdl/proceedings/greencom-ithingscpscom/2013/12OmNvk7JKB.

[353]Cfr. United Nations, *World Population Prospects 2022*, disponibile *online* su https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/wpp2022_summary_of_results.pdf

[354]Sull'*Internet of Things* nel campo dell'agricoltura, v. M. Kanderp Narayan et al, *Survey on Internet of Things and its Application in Agriculture*, in *Journal of Physics: Conference Series 1714,* 2021, pp. 5 e ss., che distinguono le applicazioni agricole basate sull'IoT a secondo della loro funzione in ambito di monitoraggio o di agricoltura di precisione.

nelle case intelligenti possono gestire i dispositivi a distanza, servendosi dei loro *smartphone* o di altri strumenti connessi ad Internet. Quello appena descritto costituisce il principale punto di forza delle *smart homes*, essendo queste state progettate per elevare i livelli di sicurezza e comfort dei loro utenti[355].

2.1.1. Le *Smart Homes*: un esempio emblematico dell'importanza del *Data Processing Agreement*

Benché le *smart homes* siano state concepite per far sentire al sicuro chi le abita, spesso accade che i dispositivi IoT ivi integrati si trasformino in delle fonti di pericolo. Questo, ad esempio, avviene quando gli *hacker* sfruttano la vulnerabilità dei sistemi IoT per installarvi dei *malware* e costituire una "*botnet*", ovvero una rete di dispositivi controllati da remoto, utilizzata per sferrare attacchi informatici[356]. Per prevenire tale fenomeno, gli utenti tendono ad adottare tecnologie volte ad assicurare la sicurezza e la privacy (*security and privacy-enhancing technologies* o S/PETs). Nello specifico, le S/PETs sono tecnologie che assolvono ad una determinata funzione, come lo scambio di messaggi, garantendo al contempo un elevato livello di protezione della privacy[357]. Le S/PETs, infatti, mirano a contenere il rischio di violazioni della privacy sia riducendo il numero di dati che il sistema

---

[355]Cfr. criticamente A. Mussab et al., *A review of smart home applications based on Internet of Things*, in *Journal of Network and Computer Applications*, 2017, n. 97, pp. 48 e ss., i quali, lungi dal limitarsi a sottolineare i benefici delle *smart homes*, ne evidenziano gli svantaggi, soprattutto relativi alla sicurezza. Infatti, gli ambienti IoT sono dotati di sistemi di sicurezza vulnerabili, che rappresentano un ostacolo alla diffusione delle case intelligenti. Una semplice interruzione di corrente nell'abitazione, ad esempio, potrebbe compromettere il funzionamento del sistema, esponendo i dispositivi *smart* a possibili attacchi esterni.

[356]Un noto esempio di *botnet* è quello che ha colpito il *provider* DNS Dyn, in cui alcuni *hacker* americani hanno adoperato il *malware* "Mirai", progettato per colpire i dispositivi IoT che operano con Linux. Sul caso, v. V. Torassa Colombero, S. Roatta, P. Lopez, *Botnets: Estado del arte y taxonomía de una amenaza sigilosa*, in *SACS - Simposio Argentino de Ciberseguridad y Ciberdefensa,* vol. X, 2024, n. 7, pp. 62 e ss.

[357]Tra le diversi tipologie di S/PETs si ravvisano cinque tecnologie principali: la crittografia omomorfa, i dati sintetici generati dall'intelligenza artificiale, il calcolo sicuro *multi-party,* l'apprendimento federato e la privacy differenziale. Per quanto riguarda la crittografia omomorfa, essa rappresenta una delle migliori tecnologie esistenti per garantire elevati livelli di privacy, poiché consente a terzi di elaborare e manipolare i dati nella loro forma criptata. In sostanza, colui che esegue l'analisi non potrà mai accedere ai dati originali. Un'altra S/PET meritevole di approfondimento è quella dei dati sintetici generati dall'intelligenza artificiale, che costituisce una delle tecnologie più versatili per la tutela della privacy. Infatti, i generatori di dati sintetici alimentati dall'IA vengono "addestrati" utilizzando dati reali e, una volta istruiti, possono creare insiemi di dati statisticamente identici, ma di dimensioni flessibili. Fra le applicazioni più comuni di dati sintetici rientrano l'anonimizzazione dei dati, l'analisi avanzata e l'apprendimento automatico. Sui diverse tipi di S/PETs, v. A. Fekete, *What are privacy enhancing technologies? The 5 best PETs for the modern tech stack*, aprile 2022, disponibile *online* su https://mostly.ai/blog/what-are-privacy-enhancing-technologies.

acquisisce, divulga e replica, sia limitando la centralizzazione e la conservazione delle informazioni[358].

Con il ricorso alle S/PETs, le relazioni tra gli attori dell'*Internet of Things* diventano ancora più complesse. Invero, tali tecnologie coinvolgono una pluralità di soggetti: sviluppatori di sistemi, fornitori di servizi, produttori di dispositivi e, infine, gli utenti, cioè i proprietari delle *smart homes* e chiunque altro adoperi le S/PETs. Considerato l'elevato numero di parti interessate, sorgono inevitabilmente dubbi riguardo agli obblighi e alle responsabilità. Ad esempio, ci si chiede se chi configura la propria *smart home* con una soluzione S/PET debba essere considerato un titolare del trattamento. In caso di risposta affermativa, ci si domanda se quel soggetto possa invocare la natura domestica della sua attività di *processing* per sottrarsi agli oneri e alle responsabilità che gravano sul *controller*[359]. A tal proposito, si è già evidenziato come il Regolamento escluda alcune ipotesi di trattamento dal proprio ambito di applicazione, tra cui quelle effettuate per ragioni puramente personali o domestiche (art. 2, par. 2, lett. c, GDPR). Al considerando n. 18, il legislatore europeo chiarisce meglio la portata di questa fattispecie, includendovi i trattamenti che non siano ricollegabili all'attività professionale. Sebbene tale esenzione possa apparire rilevante nel contesto delle *smart homes*, la sua applicabilità si riduce notevolmente se si considerano le tipologie di soggetti coinvolti. In dettaglio, non sembra che possano beneficiarne i produttori di dispositivi, né tantomeno gli sviluppatori di *software*, poiché, da un lato, hanno un coinvolgimento professionale e commerciale nell'attività; dall'altro, molti di loro non sono persone fisiche, ma giuridiche, il che preclude automaticamente l'applicazione della fattispecie in esame. Rispetto a queste categorie di attori, si pone allora una questione diversa: se essi siano congiuntamente titolari del trattamento e in che misura possano rispondere di eventuali illeciti. Ciò che è certo è che difficilmente potrebbero evitare l'applicazione del Regolamento invocando la lett. c. dell'art. 2, par. 2, GDPR.

---

[358]Un'attenta analisi del funzionamento delle S/PETs si rinviene nella relazione tenuta da S. Gürses, C. Troncoso, C. Diaz alla "*Amsterdam Privacy Conference*" del 2015, dal titolo "*Engineering Privacy by Design Reloaded*", disponibile *online* su http://carmelatroncoso.com/papers/Gurses-APC15.pdf.

[359]In questi termini, v. J. Chen et al., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption,* in *International Data Privacy Law,* vol. X, 2020, n. 4, pp. 281 e ss.

Sulla base di tali considerazioni, sembrerebbe che gli unici a poter usufruire dell'esenzione per attività personali siano gli utenti finali delle S/PETs. Tuttavia, in senso contrario, potrebbe essere letto quanto stabilito dalla Corte di Giustizia in relazione ad un dispositivo di sicurezza domestica, benché non "intelligente"[360]. Nel caso in esame, i giudici di Lussemburgo hanno dovuto pronunciarsi sull'applicabilità dell'esenzione per uso domestico ad una Televisione a Circuito Chiuso (TVCC) che, pur essendo installata nell'abitazione del convenuto, riprendeva in parte un'area pubblica[361]. A parere della Corte, nella misura in cui <<una videosorveglianza […] si estende, anche se solo parzialmente, allo spazio pubblico, e pertanto è diretta verso l'esterno della sfera privata della persona che procede al trattamento dei dati con tale modalità, essa non può essere considerata un'attività esclusivamente "personale o domestica">>[362].

Traslando questo principio alle S/PETs, si rileva come, per poter ricorrere all'art. 2, par. 2, lett. c, GDPR, occorra dimostrare che i dati raccolti tramite tali tecnologie siano utilizzati esclusivamente nella sfera privata dell'utente e della sua famiglia. A differenza delle telecamere, però, in un ambiente IoT come quello delle *smart homes* non esistono confini fisici ben definiti. Difatti, nonostante queste tecnologie mirino a tutelare lo spazio privato dell'utente, il loro impiego comporta spesso l'interazione con soggetti esterni al nucleo familiare, sia in prossimità dell'abitazione, ad esempio vicini e visitatori, sia a distanza, ad esempio altri utenti collegati al medesimo servizio. Ancor più importante, lo scopo domestico, da solo, non costituisce un fondamento giuridico sufficiente ad invocare l'esenzione in commento. In tal senso si è espressa anche la Corte di Giustizia, la quale, pur riconoscendo che le telecamere a circuito chiuso servissero solo a proteggere il convenuto e la sua famiglia, ha respinto l'applicabilità dell'esenzione per motivi domestici, indicando basi giuridiche alternative come il legittimo interesso perseguito dal *controller*[363].

---

[360]Corte di Giustizia dell'Unione Europea, 11 dicembre 2014, C-212/13, *František Ryneš contro Úřad pro ochranu osobních údajů,* in *Diritto, Mercato, Tecnologia*, 2015, n. 3, con nota di D. B. Casiere, *La videosorveglianza ad uso domestico: ambito di applicazione della direttiva europea in materia di protezione dei dati personali*.

[361]Il rinvio pregiudiziale alla Corte di Giustizia aveva ad oggetto l'art. 3, par. 2, della Direttiva 95/46 CE che, al pari dell'art. 2, par. 2, lett. c, GDPR, sottraeva all'applicazione della normativa comunitaria i trattamenti dei dati personali condotti per ragioni meramente personali o domestiche.

[362]Corte di Giustizia dell'Unione Europea, *op. ult. cit*, par. 33.

[363]Corte di Giustizia dell'Unione Europea, *op. ult. cit.,* par. 34.

Alla luce di ciò, non sembra rilevare che il proprietario di una casa intelligente utilizzi i dispositivi S/PETs unicamente per motivi personali. Al contrario, il fatto che tali tecnologie comportino la raccolta di dati personali al di fuori della sfera domestica preclude il rimando alla lett. c dell'art. 2, par. 2, GDPR. Di conseguenza, per i fruitori delle *smart homes*, l'adozione di tecnologie ideate per migliorare la sicurezza e la privacy dell'abitazione fa sì che possano essere classificati come titolari del trattamento, al pari degli altri soggetti operanti in quel settore[364]. Come anticipato, infatti, i sistemi IoT, specialmente le case intelligenti, implicano il coinvolgimento di una pluralità di attori, ciascuno con una propria funzione e, pertanto, con un diverso grado di controllo sul sistema. Gli sviluppatori, ad esempio, esercitano un controllo schematico poiché definiscono la struttura dei dati e i protocolli che regolano le comunicazioni tra le componenti del sistema, senza però poter accedere ai dati reali. I produttori dei dispositivi, invece, detengono un controllo di i*nput,* stabilendo quali dati vengono raccolti e trasmessi in rete. Gli sviluppatori di applicazioni, a loro volta, possiedono un controllo interpretativo, giacché determinano come i dati possono essere tradotti e usati concretamente. In ultimo, gli utenti dispongono di un controllo operativo, potendo scegliere quali componenti o funzionalità devono essere abilitate. Ebbene, il livello di integrazione e interdipendenza tra gli attori comporta che tutti possano essere chiamati a rispondere per un trattamento illecito dei dati[365]. Se questo è vero, è altresì vero che le diverse funzioni svolte generano asimmetrie sul piano delle risorse e dei poteri, che inevitabilmente influiscono sulla qualificazione dei soggetti come *controller* o come *processor* e, quindi, sulla ripartizione della responsabilità. Per una corretta attribuzione di quest'ultima, è necessario applicare il richiamato criterio funzionale, che consente alle parti di comprendere la natura del loro rapporto, se di contitolarità o meno. A seguito di tale analisi, le parti devono stipulare un *Data Processing Agreement*, al fine di definire in modo chiaro e inequivocabile ruoli e responsabilità.

---

[364] In posizione critica rispetto alla configurabilità dell'utilizzatore di un dispositivo domotico come *controller*, v. L. Vizzoni*, Domotica e diritto. La* Smart Home *tra regole e responsabilità*, in V. Franceschelli, E. Tosi (diretto da), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2021, pp. 81 e ss., la quale rileva che è difficile immaginare come un simile soggetto possa determinare le finalità e i mezzi del trattamento e, quindi, possa essere ricondotto alla nozione di titolare di cui all'art. 4 del GDPR. Al contrario, <<sembra possibile considerare l'utente quale interessato>> dal momento che sono i dati personali di quest'ultimo ad essere oggetto del trattamento.

[365] L'adozione di un simile approccio funzionale per distinguere il tipo di controllo esercitato dagli attori dell'IoT è stata proposta da J. Chen et al., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption*, cit., pp. 90 e ss.

In definitiva, sebbene il legislatore europeo non potesse prevedere scenari tanto complessi, sembra comunque aver fornito agli attori del trattamento strumenti adeguati ad affrontare *data processing* articolati, come quelli che caratterizzano le *smart homes*.

2.2. Profili critici della negoziazione nell'universo IoT, e non solo

Pur riconoscendo questo merito al legislatore, non si può ignorare come egli abbia, in parte, fallito nell'elaborare una normativa che si adatti alle nuove tecnologie, apparendo ciò particolarmente evidente nel contesto dell'*Internet of Things*. Al pari della Direttiva 95/46 CE, anche il GDPR presuppone che il *controller* sia la parte forte del rapporto, al quale spettano tutte le decisioni in materia di raccolta e trattamento dei dati personali. Andando ad analizzare la catena di fornitura dell'IoT, però, ci si rende conto che la realtà è molto diversa: il cliente, in qualità di *controlle*r, si rivolge ad un'azienda esterna per l'erogazione di determinati servizi che implicano il trattamento dei dati. Tale azienda agisce come *processor*, ma non solo per quel singolo *controller;* infatti, questa stipula analoghi contratti di *outsourcing* con numerosi altri clienti, operando come responsabile per ognuno di essi. Così facendo, l'azienda - *processor* diviene la parte contrattuale forte, che redige i DPA e li sottopone ai *controller* per la firma, e non viceversa. Una simile dinamica non contraddistingue solo l'IoT, ma anche un servizio ad esso strettamente connesso, il *cloud computing*[366]. A riprova di ciò, si pone il caso di Google che, in veste di fornitore di servizi *cloud,* dispone dei dati personali di migliaia di clienti, ricevendo istruzioni di trattamento dei dati da ciascuno di loro. In realtà, il processo di elaborazione di tali istruzioni è generalmente invertito, essendo i termini stabiliti dal *cloud service provider* (*data processor*) attraverso clausole che non lasciano ai propri clienti (*data controller*) margini di scelta, se non quella di accettare le condizioni di trattamento oppure rinunciare al servizio[367].

---

[366]La connessione tra i due settori deriva dal fatto che i fornitori di servizi *cloud* spesso raccolgono dati dai sensori IoT per elaborarli.

[367]Cfr. *Cloud Data Processing Addendum (Customers*), disponibile *online* su https://cloud.google.com/terms/data-processing-addendum., ove Google charisce che l'*Addendum*, il quale integra il contratto di *cloud* in essere tra le parti, è volto a regolare il trattamento dei dati derivante dal contratto principale, in relazione al quale Google agisce in qualità di *data processor*: *<<this Cloud Data Processing Addendum (including its appendices, the "Addendum") is incorporated into the Agreement(s) (as defined below) between Google and Customer. This Addendum was formerly known as the "Data Processing and Security Terms" under an Agreement for Google Cloud Platform*>>. Proseguendo nella lettura dell'*Addendum*, si rileva altresì che, sebbene il par. 5.2 sia intitolato << *Compliance with Customer's Instructions*>>, con questa clausola

Sebbene questa prassi sia comune nella società digitalizzata, è fondamentale ricordare che sono i titolari a dover garantire la conformità al GDPR[368], ragion per cui questi non possono affidarsi passivamente ai termini contrattuali standard redatti dal *processor*.

2.2.1. Conformità del *Data Processing Agreement* al GDPR. La posizione dell'autorità svedese nel caso del Comune di Salem

L'importanza di concludere DPA che soddisfino i requisiti della normativa sulla *data protection*, piuttosto che gli interessi del contraente forte, quale il *processor*, è stata ribadita anche dall'Autorità svedese per la protezione dei dati (IMY)[369]. Nel 2011, l'IMY ha esaminato l'utilizzo del servizio *cloud* "Google Apps", in particolare del calendario e della posta elettronica, da parte del consiglio comunale di Salem. Al termine della verifica, l'Autorità svedese ha ordinato al Comune di redigere un nuovo accordo sul trattamento dei dati che osservasse i criteri della legge nazionale sulla protezione dei dati. Nello specifico, il DPA doveva garantire che il responsabile non disponesse dei dati personali per scopi diversi da quelli per i quali era stato incaricato. Inoltre, l'accordo doveva specificare la procedura di restituzione e/o eliminazione dei dati una volta concluso il trattamento, affinché il *processor* non ne avesse più accesso in futuro. Da ultimo, il contratto doveva prevedere che il titolare, ossia il Comune, fosse sempre messo al corrente di eventuali sub-responsabili che dovessero intervenire nel trattamento[370].

---

il cliente autorizza Google a trattare i propri dati in conformità al contratto di *cloud computing* e all'*Addendum*, ossia in conformità ad atti predisposti dagli operatori di Google, e non dal cliente stesso.

[368]Circa l'onere di conformità al GDPR che grava sul titolare, v. P. Carey, *Data Protection: A Practical Guide to UK and EU Law*, Oxford, Oxford University Press, 2015, pp. 180 e ss.

[369]Dal 2021 il nome dell'Autorità svedese per la protezione "*Datainspektionen" è* stato modificato in "*Integritetsskyddsmyndigheten"*, o IMY. Benché all'epoca dei fatti fosse ancora in uso la denominazione precedente, per comodità espositiva ci si riferirà all'Autorità di protezione come IMY.

[370]Per un approfondimento sulla decisione dell'Autorità svedese del 2011, v. Nordic Council of Ministers, *Nordic Public Sector Cloud Computing – a discussion paper*, 2012, pp. 34 e ss., disponibile *online* su https://norden.diva-portal.org/smash/get/diva2:701433/FULLTEXT01.pdf. Nel testo, gli autori fanno presente che la Svezia non è stato il primo Paese europeo a dubitare dell'utilizzabilità del servizio *cloud* di Google nel settore pubblico; infatti, le conclusioni dell'IMY sono paragonabili alle conclusioni preliminari del caso Narvik in Norvegia (2011) e del caso Odense in Danimarca (2010).

Nel 2013, l'Autorità svedese ha analizzato il nuovo accordo tra il Comune di Salem e il *provider* Google [371], ritenendolo insoddisfacente[372]. *In prims*, l'IMY ha osservato che la clausola relativa alle finalità del trattamento era troppo ampia, poiché prevedeva soltanto che il responsabile disponesse dei dati del cliente <<*for the purposes of providing, maintaining and improving the service*>>[373]. Posta in questi termini, la clausola consentiva al *processor* di trattare i dati personali per i propri scopi, contravvenendo alla regola base del rapporto *controller-processor* secondo cui il responsabile tratta i dati nei limiti delle finalità stabilite dal titolare. L'accordo, infatti, non si discostava dai modelli di DPA comunemente adottati dai fornitori di servizi *cloud*, i quali, essendo contratti standard, non definiscono lo scopo del *data processing.* Al contrario, questi sono formulati in modo da permettere al responsabile di trattare i dati per i propri obiettivi, quali, ad esempio, la maggior diffusione o il miglioramento dei servizi *cloud* offerti. Ebbene, a parere dell'IMY, perché il DPA fosse conforme all'allora vigente normativa sulla protezione dei dati, lo scopo del trattamento doveva essere chiaramente delimitato. A tal fine, occorreva specificare quali dati personali, o quali categorie di dati personali, fossero nella disponibilità del titolare e in che misura la loro gestione fosse affidata al responsabile. Tuttavia, il contratto tra Google e il Comune di Salem non includeva queste precisazioni, pertanto non soddisfaceva i requisiti della legge sulla *data protection*[374].

In *secundis*, l'Autorità svedese ha rilevato che le condizioni contrattuali, così come erano state formulate, consentivano a Google di trattare i dati anche dopo aver ultimato la prestazione. Del resto, il DPA disponeva genericamente che <<*after termination or expiry of the Agreement, Google will delete Customer Data in accordance with the terms of the Agreement*>>[375]. Secondo l'IMY, la succitata previsione sui tempi di cancellazione non era compatibile con la legge nazionale sulla protezione dei dati, poiché non indicava per quanto tempo il fornitore di servizi

---

[371]La decisione dell'Autorità svedese teneva conto sia del contratto principale, Google Apps *Enterprise*, che dell'*Addendum*, ovvero l'accordo sul trattamento dei dati personali.

[372]Così M. Ricknäs, *Google Apps deal disallowed by Swedish data regulator*, 10 giugno 2013, disponibile *online* su https://www.pcworld.com/article/452338/google-apps-deal-disallowed-by-swedish-data-regulator.html.

[373]*Integritetsskyddsmyndigheten* (IMY), *Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011,* 31 maggio 2013, par. 1.2, disponibile *online* su https://www.imy.se/globalassets/dokument/beslut/2013-/2013-05-31-salems-kommun.pdf.

[374]IMY, *op. ult. cit.*, par. 1.3.

[375]*Data Processing Amendment to* Google Apps *Enterprise Agreement*, 14 novembre 2012, par. 7, disponibile *online* su https://workspace.google.com/terms/11142012/dpa_terms/.

avrebbe conservato i dati allo scadere dell'accordo. Al fine di conformarsi alla normativa vigente, il DPA avrebbe dovuto individuare almeno un periodo massimo per la conservazione dei dati[376].

Infine, l'Autorità svedese contestava le modalità con cui Google poteva rivolgersi ad un soggetto terzo, *sub-processor*, per affidargli parte del trattamento. Secondo l'accordo, il *provider* avrebbe dovuto semplicemente fornire un elenco dei potenziali sub-responsabili, senza specificare chi avrebbe effettivamente collaborato. In questo modo, il DPA disattendeva la disciplina vigente che imponeva al titolare di garantire agli interessati l'esercizio dei loro diritti. A tal fine, era necessario che il *controller* conoscesse l'identità dei responsabili e sub-responsabili, nonché la loro ubicazione, condizione che tuttavia non poteva essere soddisfatta con la soluzione prevista dall'accordo. L'elenco, infatti, non garantiva che il *controller* fosse informato su chi eseguiva il trattamento, né tantomeno su dove si svolgeva[377].

In ultima analisi, la decisione dimostra che il titolare non deve accettare le condizioni contrattuali standard senza valutare il caso concreto; altrimenti, rischia di trovarsi in una posizione analoga a quella del Comune di Salem, con un *processor* che detta le istruzioni del trattamento e dispone dei dati per perseguire i propri fini[378].

2.3. Il *Cloud of Things*: una pluralità di contratti e di contraenti

Come si è precedentemente accennato, pur trattandosi di tecnologie autonome, il *cloud computing* e l'*Internet of Things* interagiscono spesso tra di loro, fino a costituire un nuovo paradigma: il *Cloud of Things*, o CoT.

In passato, la dottrina aveva escluso ogni legame tra le due tecnologie, ritenendo che la componente materiale della "*Thing*" fosse del tutto estranea alla sfera del *cloud computing;* pertanto, il *cloud* e l'IoT erano stati analizzati

[376]IMY, *Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011,* cit., par. 2.3 e ss., la quale precisa che l'indicazione di un periodo massimo relativamente lungo è accettabile a patto che il responsabile possa servirsi dei dati unicamente per motivi di sicurezza, o nell'ambito della cancellazione dei dati in questione.
[377]IMY, *op. ult. cit.*, par. 3.3.
[378]Per un commento alla decisione dell'Autorità svedese, v. L. Tung, *Sweden tells council to stop using* Google Apps, 14 giugno 2013, disponibile *online* su https://www.zdnet.com/article/sweden-tells-council-to-stop-using-google-apps/.

separatamente[379]. Sebbene tali tecnologie abbiano avuto un'evoluzione indipendente, nel tempo è emersa la consapevolezza che non devono necessariamente rimanere distinte, poiché l'una può trarre beneficio dall'altra. Da un lato, l'IoT può sfruttare la capacità di archiviazione illimitata del *cloud* per compensare i propri limiti di "memoria"; dall'altro, il *cloud* può estendere il proprio ambito di applicazione al mondo fisico, grazie all'interconnessione con gli oggetti intelligenti dell'IoT[380]. Un esempio significativo dell'efficienza del CoT è rappresentato dal "ClouT", un progetto di ricerca condotto da un partenariato di aziende europee e giapponesi, in collaborazione con università e centri di ricerca. L'obiettivo del progetto è sviluppare servizi innovativi per le città e i loro abitanti, attraverso applicazioni basate *sull'Internet of Things* e supportate dalle infrastrutture *cloud.* Tali applicazioni sono volte a migliorare il trasporto pubblico, nonché a coinvolgere maggiormente i cittadini nella gestione urbana (ad es. permettendo loro di segnalare situazioni di interesse pubblico tramite fotografie), come pure ad agevolare il mantenimento dell'ordine pubblico[381].

Grazie al progetto italo-giapponese, è possibile cogliere a pieno la portata del paradigma "*Cloud of Things"*, che si riferisce a tutti gli ecosistemi in cui gli oggetti "comunicano" tra di loro per mezzo dei servizi *cloud*[382]. Malgrado ciò, molti aspetti di questo sistema risultano poco chiari a coloro che vi si approcciano, ostacolandone la diffusione. D'altronde, il *Cloud of Things* si contraddistingue per la sua complessità tecnica, in quanto le tecnologie coinvolte sono spesso sconosciute al grande pubblico, il quale, se di solito comprende il significato di *cloud computing*, difficilmente conosce la *Radio Frequency Identification* (RFID), la *Near-Field Communication* (NFC)[383] o il Bluetooth a bassa energia (LEB). Le

---

[379]Tra tutti, v. R.H. Weber, R. Weber, *Internet of Things. Legal Perspectives*, Berlino, Springer, 2010, pp. 17 e ss.

[380]Una disamina dei benefici che l'IoT può apportare al *cloud*, e viceversa, si rinviene nella relazione tenuta da A. Botta et al. alla "*International Conference on Future Internet of Things and Cloud Barcelona"* del 2014, dal titolo *"On the Integration of Cloud Computing and Internet of Things",* pp. 23 e ss., disponibile *online* su https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6984170.

[381]Nello specifico, il "ClouT" mira a raggiungere i seguenti risultati: realizzare delle vere e proprie città intelligenti, dotate di infrastrutture capaci di elaborare e archiviare un elevato numero di dati provenienti da cose e persone; sviluppare un sistema di piattaforme per facilitare l'implementazione e la diffusione di applicazioni IoT. Sul punto, cfr. *ClouT, a joint European-Japanese project,* disponibil*e online* su https://clout-project.eu/home2/.

[382]Così W. Kuan Hon, C. Millard, J. Singh, *Twenty Legal Considerations for Clouds of Things,* in *Legal Studies Research Paper,* 2016, n. 216, pp. 9 e ss.

[383]Le tecnologie RFID e NFC sono alla base del CoT poiché rendono possibile un flusso di dati tra dispositivi. Tuttavia, esse presentano delle differenze significative, primo fra tutti il *modus operandi:*

difficoltà tecniche non riguardano solo gli utenti, ma anche gli esperti del settore stanno ancora studiando fattori del CoT che necessitano di essere perfezionati. Tra questi, si segnalano: i vincoli *hardware*, come interfacce di misura ridotta, autonomia energetica limitata, difficoltà nella crittografia; la "*multitenancy*", ovvero la titolarità condivisa degli oggetti che può determinare usi conflittuali degli stessi; l'impossibilità di tracciare i dati lungo l'intero flusso sistemico, che è essenziale per assicurarne l'integrità[384].

A tutto questo si aggiungono le problematiche derivanti dalla "giungla normativa" che connota la materia, regolata da una miriade di atti come pareri, linee guida, comunicazioni, nessuno dei quali vincolante. Non a caso, la Commissione Europea, prima della diffusione del CoT, aveva già impiegato la locuzione <<*jungle of standards*>>[385] per riferirsi alla situazione esistente nell'ambito del *cloud computing*. In tale contesto, la proliferazione di standard rappresentava, per l'Istituzione, uno dei principali ostacoli all'adozione del *cloud*, con conseguenze significative per tutte le parti interessate, specialmente per le piccole e medie imprese e i consumatori[386].

Il mondo del *Cloud of Things*, oltre ad essere affollato da una pluralità di atti normativi, è popolato da una moltitudine di contratti. Ciò è emerso da un recente studio condotto tramite una ricerca empirica sulla documentazione legale di Nest Inc, un'azienda di CoT che fornisce termostati, allarmi antifumo e videocamere[387].

---

le RFID richiedono l'uso di un tag e di un lettore, di cui invece non necessitano gli strumenti NFC. Diversamente dalle prime, però, le tecnologie NFC utilizzano onde a corto raggio; quindi, consentono lo scambio di dati solo tra dispositivi vicini. Sul funzionamento e sulle aree di diffusione di tali tecnologie, v. S. Jain, P. S. Halgaonkar, V.M. Wadhai, *Review of RFID, NFC Technology and Its Applications,* in *International Journal of Engineering Research & Technology*, vol. III, 2014, n. 2.

[384]V. le osservazioni di S. Haq, A. Bashir, S. Sholla, *Cloud of Things: Architecture, Research Challenges, Security Threats, Mechanisms and Open Challenges*, in *Jordanian Journal of Computers and Information Technology*, vol. VI, 2020, n. 4, pp. 420 e ss., i quali rilevano che l'integrazione tra il *cloud* e l'IoT pone molte sfide tecniche ancora da risolvere, a partire dalla necessità di sviluppare piattaforme e sistemi operativi *ad hoc* per queste nuove applicazioni.

[385]Commissione Europea, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Unleashing the Potential of Cloud Computing in Europe*", COM (2012) 529 final, 27 settembre 2012, par. 3, disponibile *online* su https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0529.

[386]Rispetto alle affermazioni della Commissione, v. le considerazioni critiche di N. Gleeson, I. Walden, "*It's a jungle out there"?: Cloud computing, standards and the law*", in *European Journal of Law and Technology,* vol. V, 2014, n. 2, pp. 21 e ss., i quali escludono che la proliferazione degli standard sia necessariamente sintomatica di un problema per il settore *cloud*, essendo piuttosto il riflesso della varietà e della complessità delle tecnologie che compongono il sistema.

[387]Cfr. G. Noto La Diega, I. Walden*, Contracting for the 'Internet of Things': Looking into the Nest,* in *Queen Mary School of Law Legal Studies Research Paper,* 2016, n. 219.

Lo studio ha dimostrato che per un unico "semplice" prodotto esistono una miriade di contratti, la cui lettura può risultare ostica per almeno quattro motivi. In primo luogo, la loro formulazione include una vasta gamma di termini tecnologici, sconosciuti ai più. In secondo luogo, molti di questi contratti sono stati redatti considerando i precedenti stadi dello sviluppo tecnologico, e quindi non si adattano perfettamente alla situazione attuale. In terzo luogo, la versione europea dei contratti spesso riproduce fedelmente quella originale statunitense, senza tener conto del diverso ordinamento giuridico in cui si utilizzano. Infine, il mercato digitale in cui questi contratti si applicano presenta una struttura complessa, che rende complicato individuare tutti gli atti realmente rilevanti per il caso specifico[388].

L'ultima criticità riguarda gli attori del CoT, poiché tale tecnologia coinvolge un numero elevato di soggetti, legati da rapporti contrattuali ed extracontrattuali. Tra questi, un ruolo di particolare rilevanza è rivestito dall'utente finale, il quale è il principale interessato e, talvolta, anche il responsabile del trattamento. A dire il vero, sarebbe più appropriato fare riferimento agli utenti finali al plurale, dato che la *multitenancy* è una caratteristica sia del *cloud computing,* che dell'IoT. Infatti, colui che stipula l'accordo di CoT potrebbe non essere l'unico ad usufruirne, dal momento che la componente materiale, ossia la "*Thing*", può essere utilizzata dai membri della famiglia, da ospiti temporanei, amici, dipendenti, ecc. Oltre ad influire sul numero degli utenti, la "Cosa" determina l'intervento di un altro soggetto nella catena di fornitura CoT: il produttore. Ancora una volta, è preferibile riferirsi a questa figura al plurale, dato che il processo di produzione richiede l'apporto di diversi sviluppatori, ciascuno impegnato nella realizzazione delle varie componenti della "*Thing*", compresi *hardware* e *software*. Il paradigma CoT, però, non si riduce solo agli elementi dell'*hardware* e al *software*, ma si estende anche ai servizi, la cui erogazione implica l'intervento di figure diverse rispetto a quelle elencate, come il *cloud provider* responsabile dell'archiviazione.

[388]Tra gli altri aspetti, lo studio citato rivela che il consumatore di un prodotto Nest, per avere un quadro completo dei diritti ed obblighi ad esso connessi, dovrebbe consultare almeno cinque diversi documenti: i termini e le condizioni di vendita con "Nest Labs (Europe) Ltd"; la garanzia limitata con "Nest Labs (Europe) Ltd"; l'informativa sulla privacy per le informazioni acquisite durante il funzionamento dei prodotti e dei servizi Nest; l'informativa sulla privacy per le informazioni raccolte attraverso i siti web, compreso il negozio online, e la policy sulla sicurezza.

Per completare il quadro della catena di fornitura, devono essere altresì menzionati lo sviluppatore del sito web e i gestori delle piattaforme di eCommerce[389].

Come ogni contesto che coinvolge più soggetti, nella catena di approvvigionamento del *Clouds of Things* potrebbe essere difficile identificare titolari, co-titolari, responsabili e sub-responsabili in relazione a ciascuno specifico trattamento. Tuttavia, è fondamentale comprendere quale attore del *data processing* riveste il ruolo di *controller* e quale di *processor,* essendo ciò strettamente correlato alla ripartizione di responsabilità tra le parti. Attualmente, i regolatori sembrano "discriminare" il settore *cloud,* giacché tendono a qualificare i fornitori di servizi come responsabili del trattamento, benché l'equivalente non-*cloud* non sia reputato tale. Si pensi, ad esempio, alla vendita di un computer: in questo caso, l'acquirente è il titolare del trattamento dei dati che effettua con il dispositivo, mentre il venditore non assume il ruolo di responsabile. Durante l'utilizzo del computer, infatti, è esclusivamente il cliente a trattare i dati. Il venditore, dal canto suo, dispone dei dati relativi alla vendita e, limitatamente ad essi, potrebbe essere qualificato come *controller*, ma non come *processor*. Rispetto a questa fattispecie, il *cloud computing* si differenzi per il modo in cui i clienti accedono alle risorse fornite, da remoto, e per l'uso della virtualizzazione. Eppure, il fatto che gli utenti usufruiscano del servizio tramite internet, anziché recarsi fisicamente in un punto vendita, non rende automaticamente il *provider* un responsabile del trattamento. Del resto, indipendentemente da come ottiene la risorsa, è sempre il cliente a disporre dei dati[390].

Se tale approccio "discriminatorio" fosse esteso al *Clouds of Things*, molti attori del trattamento potrebbero essere classificati come responsabili, o persino titolari, nonostante alcuni di loro siano solo fornitori di servizi complementari.

---

[389]Sulla pluralità di attori coinvolti nel *Cloud of Things*, v. G. Noto La Diega, *Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom,* in *Journal of Law & Economic Regulation,* vol. IX, 2016, n. 1, pp. 79 e ss.

[390]In questo senso, v. W. Kuan Hon, C. Millard, I. Walden, *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing*, in *International Data Privacy Law,* 2012, n. 1, pp. 14 e ss., i quali, a sostegno del loro ragionamento, analizzano l'ipotesi del noleggio di uno strumento informatico, pervenendo alle medesime conclusioni della vendita. Infatti, anche nel caso in cui venisse utilizzato un *software* installato dal fornitore, l'unico a trattare i dati sarebbe colui che noleggia il dispositivo. Solo se si fosse impegnato a garantire la manutenzione dell'*hardware* o del *software*, il professionista potrebbe accedere incidentalmente ai dati memorizzati nel dispositivo. Tuttavia, una simile eventualità non sembrerebbe sufficiente a qualificare il fornitore come responsabile del trattamento.

Questo potrebbe aumentare i costi e i tempi di commercializzazione della tecnologia CoT, oltre ad avere un impatto negativo sull'innovazione[391].

3. Il *Cloud Computing* e la distribuzione dei ruoli alla luce del GDPR

Prima ancora del CoT, il tema della corretta attribuzione di funzioni non può non riguardare le fattispecie che ne costituiscono il fondamento, in particolare il *cloud computing service*. Come anticipato, tale servizio consente l'accesso remoto a risorse informatiche, quali *server* e *storage*[392]. Per usufruirne, l'utente, o *cloud consumer,* conclude un contratto con il *cloud service provider,* il quale può, a sua volta, avvalersi di altri *sub-provider* per erogare parte del servizio. Siffatta contrattazione su più livelli è una pratica comune nell'ambito del *cloud*, al punto che, in alcuni casi, il contratto riconosce espressamente al fornitore la facoltà di rivolgersi a terzi; in altri, tale diritto viene fatto implicitamente derivare dalla natura del servizio[393]. A prescindere dal tipo di formulazione, è indubbio che il ricorso a soggetti esterni non riguarda solo i *provider* minori, ma anche i grandi colossi del settore, come Dropbox, che nelle proprie condizioni contrattuali ammette di affidare a terze parti alcuni aspetti del servizio[394].

Intervenendo nell'erogazione della prestazione, questi soggetti partecipano altresì al trattamento di dati che contraddistingue il *cloud*. Per questo motivo, è importante stabilire se rivestono il ruolo di *controller* o *processor*, al fine di ripartire correttamente le rispettive responsabilità.

---

[391]Cfr. W. Kuan Hon, C. Millard, J. Singh, *Twenty Legal Considerations for Clouds of Things,* in *Legal Studies Research Paper,* cit., pp. 22 e ss.

[392]Così National Institute of Standards and Technology (NIST), *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, 2011, pp. 2 e ss., disponibile *online* su https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, che, oltre a fornire una definizione di *cloud computing*, ne individua le principali caratteristiche: autonoma allocazione delle risorse da parte dell'utente; ampio accesso alla rete tramite una varietà di strumenti come telefoni, computer ecc., *multitenancy* ed, infine, capacità dei sistemi *cloud* di monitorare e ottimizzare l'uso delle risorse attraverso meccanismi di misurazione adeguati al tipo di servizio.

[393]Sulla figura del *sub-provider*, v. United Nations Commission on International Trade Law (UNCITRAL*), Notes on the Main Issues of Cloud Computing Contracts*, 2019, pp. 30 e ss., disponibile *online* su https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09103_eng.pdf, che evidenzia come il *sub-provider* non sia necessariamente lo stesso per tutta la durata del contratto, potendo questi variare a seconda delle esigenze del fornitore principale.

[394] Per un'analisi approfondita sui termini contrattuali di Dropbox e di altri grandi fornitori di servizi *cloud*, v. i risultati dello studio condotto da K. Stylianou, J. Venturini, N. Zingales, *Protecting user privacy in the Cloud: an analysis of terms of service*, in *European Journal of Law and Technology*, vol. VI, 2015, n. 3.

3.1. *Cloud Consumer* e *Cloud Service Provider*, titolari o responsabili del trattamento?

Sin dalle prime manifestazione del *cloud computing*, il Gruppo di lavoro per la protezione dei dati personali (Art. 29) ha tentato di inquadrare i suoi attori nell'ambito del *data processing*[395]. Analizzando il fenomeno del *cloud* alla luce della Direttiva 95/46 CE, il Gruppo perveniva alla conclusione che il cliente era il titolare del trattamento, poiché questi determinava le finalità del trattamento e decideva se esternalizzare il processo. Al contrario, il *cloud provider,* fornendo i mezzi e la piattaforma per conto del *cloud client*, era da ritenere il responsabile del trattamento, giacché corrispondeva alla figura di *data processor* delineata dalla Direttiva. A queste ipotesi, il Gruppo di lavoro ne affiancava una residuale, ossia quando il fornitore di servizi *cloud* trattava i dati per i propri scopi, assumendo la veste di titolare. Nella maggior parte dei casi, però, era il cliente a determinare le finalità per cui il *provide*r avrebbe dovuto disporre dei dati. Pertanto, il fornitore non era altro che un "appaltatore" nei confronti del *cloud client*[396].

La dottrina dell'epoca ha avvalorato le considerazioni del Gruppo, analizzando le relazioni che intercorrevano tra cliente e fornitore nelle diverse tipologie di *cloud computing service.* Prendendo le mosse dal *software as a service* (SaaS), essa evidenziava come, in relazione a suddetta forma di *cloud*, dovesse preliminarmente distinguersi: una prima fase di elaborazione dei dati ad opera del *software*; una seconda fase di gestione dei dati elaborati (memorizzazione o *storage*), che costituiva il trattamento dei dati vero e proprio. In merito a questo tipo di *cloud,* veniva altresì fatto notare che era il cliente a decidere quali dati immettere nel s*oftware* e a quale scopo, mentre il fornitore doveva limitarsi ad agire secondo le sue indicazioni. In ragione di ciò, l'uno era considerato il titolare del trattamento, l'altro il responsabile. Se la qualificazione *controller – cloud client* e *processor –*

---

[395]Il Gruppo di lavoro per la protezione dei dati (art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del trattamento"* (WP 169), cit., par. 3.2, aveva già affrontato il problema in relazione al precursore del *cloud computing service*: il servizio di *hosting* su Internet. In proposito, il Gruppo aveva chiarito che <<un *provider* di servizi Internet (ISP) che fornisce servizi di hosting è in linea di principio un incaricato del trattamento [responsabile] per i dati personali pubblicati on-line dai suoi clienti, che si rivolgono a lui per l'*hosting* e la manutenzione del loro sito web>>.

[396]Cfr. Gruppo di lavoro per la protezione dei dati (art. 29), *Parere 05/2012 sul* cloud computing *(WP 196*), cit., par. 3.3.1., il quale rileva come, a prescindere dalla qualificazione del *provider,* sia indispensabile stabilire chi, tra il cliente e il fornitore, debba rispondere per eventuali inosservanze della normativa sulla *data protection,* e in quale misura. In caso contrario, potrebbe verificarsi un <<conflitto negativo di competenze>>, con il rischio che la disposizione sugli oneri e i diritti delle parti contenute nella Direttiva, e oggi nel GDPR, non siano correttamente applicate.

cloud provider valeva per il SaaS*,* essa era applicabile *a fortiori* alla fattispecie del *cloud infrastructure as a service* (IaaS), dal momento che questo aveva ad oggetto esclusivamente l'attività di *storage* riscontrata nell'altro modello. Infine, occorre evidenziare come gli stessi argomenti venissero utilizzati anche per il *platform as a service* (PaaS). La dottrina, infatti, sosteneva che tale forma di *cloud,* pur avendo delle proprie peculiarità, come permettere l'uso simultaneo di più applicativi, nonché favorire lo sviluppo di un s*oftware* piuttosto che offrire un prodotto finito, comportava un trattamento dei dati pressoché analogo alle altre modalità del servizio. Del resto, lo scopo del trattamento rimaneva quello di memorizzare i dati necessari al buon andamento del *software*[397].

Benché facesse riferimento alla disciplina previgente, la prospettata distribuzione dei ruoli, *client* – titolare e *provider* – responsabile, sembra potersi riscontrare anche in vigenza del Regolamento. Ciò è quanto emerge dai termini di servizio (ToS) dei principali attori del *cloud computing service*, recentemente esaminati da un gruppo di studiosi anglosassoni[398]. Questi ultimi hanno rilevato come gran parte dei *cloud provider* includa nei loro ToS disposizioni che disciplinano esplicitamente i ruoli di titolare e/o responsabile, in conformità con quanto previsto dal GDPR. I ToS di Tencent Cloud, ad esempio, chiariscono che, rispetto ai dati archiviati dagli utenti, la compagnia fornitrice agisce in qualità di *data processor*; di conseguenza, la titolarità del trattamento è da ricondursi agli utenti[399]. Un approccio simile è adottato anche dagli altri *cloud provider*, quali Alibaba Cloud, ADrive e Mozy, In particolare, il primo ha optato per dei temini di servizio che rimandano al GDPR, laddove stabiliscono che il fornitore assume la veste di *controller* quando raccoglie e utilizza i dati per i propri scopi; diversamente, opera come *processor*[400].

---

[397]Tra tutti, v. A. Mantelero, *Responsabilità aquiliana per uso della Rete e responsabilità del* provider*,* in F. Delfini, G. Finocchiaro (a cura di), *Diritto dell'informatica*, cit., pp. 823 e ss.

[398]Cfr. D. Kamarinou, C. Millard, F. Turton, *'Responsibilities of Controllers and Processors of Personal Data in Clouds',* in C. Millard (a cura di), *Cloud Computing Law,* Oxford, Oxford University Press, 2021, pp. 11 e ss.

[399]Cfr. Tencent Cloud, *Terms and Policies: Privacy Policy*, 2025, pp. 5 e ss., disponibile *online* su https://www.tencentcloud.com/document/product/301/17345, ove si informa il cliente che <<*you* [il cliente] *are the data controller of Content* […]. *At all times, we [Tencent Cloud] act as a service provider to you, and process data on your behalf*>>.

[400]Cfr. Alibaba Cloud, *International Website Privacy Policy. EEA and UK Addendum***,** 2024, disponibile *online* su https://www.alibabacloud.com/help/en/legal/latest/alibaba-cloud-international-website-privacy-policy, dove, per chiarire quand'è che il *provider* agisce come titolare, si riporta il seguente esempio: <<*when customers of our Cloud Services register an account with us or provide contact information in order to receive customer support, we are the controller of that data*>>.

Sebbene quella appena descritta sia l'impostazione maggioritaria, alcuni *provider* hanno scelta una soluzione differente per i loro ToS. Tra questi anche il *cloud provider* Tresorit, che attribuisce la funzione di titolare o di responsabile a seconda del cliente con cui si relaziona. Qualora questo sia di natura individuale, il *provider* tratta i suoi dati in qualità di titolare, potendo decidere sia i mezzi, che lo scopo del trattamento. Viceversa, se il cliente ha una struttura aziendale, il fornitore dispone dei dati in veste di *processor*, agendo in conformità alle istruzioni del cliente[401]. Un criterio ancora diverso è stato impiegato da Apple ICloud per i propri termini di servizio; difatti, questo assegna lo status di titolare e di responsabile a enti differenti: "*Apple Distribution International"*, con sede in Irlanda, è il titolare del trattamento; "*Apple Inc*.", avente sede nello Stato americano del Delaware, è il responsabile[402].

Salvo rare eccezioni, quindi, il trattamento dei dati effettuato dagli attori del *cloud* riflette la ripartizione dei ruoli ipotizzata dal Gruppo di lavoro per la protezione dei dati personali (Art. 29). Se questo è e vero, è altresì vero che il GDPR ha dedicato un articolo *ad hoc* (art. 26 GDPR) alla regolazione di un ulteriore rapporto, quello tra i contitolari del trattamento. Affinché due soggetti siano identificati come *joint controllers*, è necessario che condividano sia le finalità sia i mezzi del trattamento. Questa condizione può sussistere anche quando l'unico scopo comune sia l'interesse economico al trattamento dei dati. Dunque, non sono circostanze ostative alla contitolarità né l'accesso a tipologie differenti di dati, né l'intervento dell'uno e dell'altro in fasi diverse del *data processing*, né tantomeno l'esistenza di uno squilibrio nell'effettivo controllo sui mezzi di trattamento[403]. D'altronde, un'interpretazione in senso ampio della contitolarità è stata fornita dalla Corte di Giustizia dell'Unione Europea nel caso *Wirtschaftsakademie* [404].

---

[401]Cfr. Tresorit, *eSign Privacy Notice*, 2024, disponibile *online* su https://tresorit.com/legal/esign-specific-privacy-policy, ove si stabilisce che <<*if your account is part of a Business Subscription – in accordance with section 5 of our Terms of Service, […] the ultimate decisions regarding your personal data will be made by the relevant organization. In such case, your company will be considered as a controller and Tresorit will act as a processor, acting upon the instructions of such organization*>>.

[402]Cfr. Apple ICloud, *Legal*, 2024, disponibile *online* su https://www.apple.com/legal/internet-services/icloud/.

[403]In questi termini, v Kamarinou, C. Millard, F. Turton, *'Responsibilities of Controllers and Processors of Personal Data in Clouds'*, cit., pp. 18 e ss, i quali, tuttavia, evidenziano come un approccio vago alla contitolarità possa avere risvolti negativi per l'interpretazione delle norme che regolano il *cloud computing.*

[404]Corte di Giustizia dell'Unione Europea, 5 giugno 2018, C-210/16*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, disponibile *online* su

3.1.1. Il caso *Wirtschaftsakademie*

La pronuncia in esame deriva da un rinvio pregiudiziale del Tribunale amministrativo federale tedesco *(Bundesverwaltungsgericht*), presentato nell'ambito del procedimento tra l'autorità di protezione dei dati dello *Schleswig-Holstein* (ULD) e la "*Wirtschaftsakademie"*, una società privata che operava nel campo della formazione. Tale società sponsorizzava i propri servizi attraverso una *fan page* ospitata dalla piattaforma Facebook. Oltre a utilizzare lo spazio sul *social network*, la *Wirtschaftsakademie* si avvaleva di un altro servizio offerto dalla piattaforma*:* Facebook Insights. Quest'ultimo consentiva alla società di ottenere informazioni statistiche anonime sui visitatori della *fan page*. A tal fine, venivano installati *cookie*[405] sui dispositivi degli utenti, che rimanevano attivi per i successivi due anni; di conseguenza, ogni volta che il visitatore accedeva alla pagina *online*, i suoi dati venivano trasmessi ai *cookie*. A fronte di questa pratica, l'ULD lamentava che gli utenti non erano stati informati del trattamento dei propri dati né da parte di Facebook, né dalla *Wirtschaftsakademie*. Pertanto, l'autorità per la protezione dei dati aveva ordinato alla società educativa di disattivare la *fan page.* A quel punto, la *Wirtschaftsakademie* aveva impugnato il provvedimento, sostenendo di non essere responsabile dell'installazione dei *cookie* sui dispositivi degli utenti, e tantomeno del successivo trattamento dei dati da parte di Facebook. Il ricorso era stato accolto dal Tribunale amministrativo, che aveva annullato la decisione. L'annullamento era stato poi confermato in sede di appello, costringendo l'ULD ad adire la *Bundesverwaltungsgericht*. Invero, l'autorità per la protezione dei dati sosteneva che la *Wirtschaftsakademie* non poteva essere esonerata da ogni responsabilità, poiché questa non solo aveva contribuito attivamente alla raccolta dei dati, ma aveva beneficiato del loro trattamento grazie a Facebook Insights. Appresi i fatti, la *Bundesverwaltungsgericht* aveva ritenuto di dover sottoporre la questione alla Corte di Giustizia, chiedendole, tra i vari quesiti, se la

https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=IT.

[405]Sul funzionamento dei *cookie*, v. W. T. Harding, A. J. Reed, R. L. Gray, *Cookies and Web Bugs: What They Are and How They Work Together,* in R. Herold (a cura di), *The Privacy Papers*, Boca Raton, Auerbach Publications, 2001, pp. 351 e ss.

*Wirtschaftsakademi*e potesse essere considerata responsabile per la violazione della legge sulla protezione dei dati (quesiti 1 e 2)[406].

Prima di procedere all'analisi della pronuncia, occorre premettere che i giudici di Lussemburgo, nel caso di specie, facevano riferimento alla Direttiva 95/46 CE. Malgrado ciò, la sentenza ha ancora una notevole rilevanza in materia di trattamento dei dati, specialmente per quanto riguarda la qualificazione degli attori coinvolti. Infatti, sebbene il Regolamento abbia disciplinato in maniera dettagliata la figura del contitolare, nonché il rapporto che egli ha con il titolare, ha preservato l'impostazione di base della Direttiva[407].

Passando ad esaminare il contenuto della decisione, si rileva come la Corte abbia inizialmente sottolineato che il concetto di "titolare del trattamento"[408] è definito dalla normativa in modo ampio, al fine di garantire una tutela effettiva degli interessati. Successivamente, essa ha osservato che la formulazione della Direttiva, rimasta sostanzialmente invariata all'articolo 4, par. 7, del GDPR, non circoscrive il titolare ad un unico soggetto; al contrario, essa può riguardare una pluralità di enti che partecipano al trattamento, ciascuno dei quali è tenuto a rispettare la disciplina sulla protezione dei dati. Dopo queste premesse, la Corte ha stabilito che, in relazione ai dati degli utenti della *fan page*, le finalità e i mezzi del trattamento erano determinati principalmente da Facebook Inc[409] e Facebook Ireland, i quali agivano in qualità di *data controller* (par. 30). Quanto al ruolo della *Wirtschaftsakademi*e, invece, i giudici hanno constatato che gli amministratori della pagina, per accedere ai servizi del *social network*, avevano accettato i termini d'uso, inclusa la politica sui *cookie* (par. 31). Così facendo, essi avevano accordato a Facebook il "permesso" di installare *cookie* nei dispositivi dei visitatori della *fan page*, indipendentemente dal fatto che il visitatore avesse o meno un *account* sul *social* (par. 35). Inoltre, gli amministratori avevano ottenuto da Facebook statistiche

[406]Per approfondimenti sulla vicenda processuale, v. O. Lynskey, *Another Turn of the Screw? The 'Facebook Fanpages' judgment*, in *European Law Blog*, 2018, disponible *online* su https://www.europeanlawblog.eu/pub/another-turn-of-the-screw-the-facebook-fanpages-judgment/release/1.

[407]Così G.M. Riccio, *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy,* in *Nuova Giurisprudenza Civile Commentata*, 2018, n. 12, pp. 1805 e ss.

[408]La versione italiana della sentenza si riferisce al *controller* come al "responsabile del trattamento", essendo questa la traduzione del termine adottata in quegli anni.

[409]All'epoca dei fatti la società portava ancora il nome di "Facebook Inc.", modificato in "Meta Inc." nel 2022. Tuttavia, le piattaforme gestite dalla holding hanno mantenuto le loro denominazioni originali (Facebook, Instagram ecc.).

elaborate sui dati dei visitatori della *fan page*, grazie alle quali avevano conosciuto le preferenze degli utenti e adattato il contenuto della pagina. Riguardo ai dati utilizzati per le statistiche, la Corte ha evidenziato che Facebook metteva a disposizione degli amministratori dei filtri, di cui essi si servivano per individuare le categorie di utenti le cui informazioni sarebbero state raccolte tramite *cookie* (par. 36). In particolare, la società poteva chiedere di ricevere, <<e, quindi, chiedere che [fossero] trattati>>[410] specifici dati demografici relativi all'età, lo stile di vita, le abitudini di spesa, ed altri ancora, che poi le venivano trasmessi in forma anonima. Alla luce di tali considerazioni, la Corte ha evidenziato come la *Wirtschaftsakademie,* definendo i parametri del *data processing,* ne determinasse anche lo scopo, divenendo così un contitolare del trattamento (par. 39). In senso opposto, non deponeva la circostanza che la società avesse accesso soltanto alla versione anonimizzata dei dati, perché <<la direttiva 95/46 non impone che, qualora vi sia una responsabilità congiunta di più operatori per un medesimo trattamento, ciascuno abbia accesso ai dati personali interessati>>[411]. Tantomeno, il ricorso ad una piattaforma esterna esentava la società dal rispetto della normativa sulla *data protection* (parr. 40 e 41). Benché Facebook e la società tedesca condividessero la titolarità del trattamento, ciò non implicava necessariamente una responsabilità paritaria delle parti. Del resto, i contitolari restano tali anche se intervengono in momenti diversi del trattamento o incidono sul procedimento in modo differente, con tutte le conseguenze che ne derivano per l'attribuzione della responsabilità (par. 43).

Da tale disamina si evince come la Corte di Giustizia abbia sposato un'interpretazione estensiva della nozione di contitolare, riconoscendo la configurabilità della *joint controllership* anche quando un titolare non abbia accesso alla totalità dei dati trattati, né partecipi a tutte le fasi del trattamento. Eppure, la pronuncia sembra tralasciare un elemento fondamentale, che potrebbe condurre a conclusioni differenti. La stessa Corte, infatti, chiarisce che i dati trattati dalla *Wirtschaftsakademie* sono anonimi, non potendo la società risalire in alcun modo agli interessati. Secondo quanto stabilito sia alla Direttiva che dal Regolamento, il trattamento di dati anonimi è estraneo all'applicazione della disciplina sulla

[410]Corte di Giustizia dell'Unione Europea, 5 giugno 2018, C-210/16, cit, par. 37.
[411]Corte di Giustizia dell'Unione Europea, *op. ult. cit.*, par. 38.

protezione dei dati[412]. In presenza di un simile principio, non si comprende come il testo della Direttiva, e successivamente del GDPR, possa essere ritenuto applicabile alla *Wirtschaftsakademie*, dal momento che gli unici dati da essa trattati, ossia quelli ricevuti da Facebook, erano anonimi[413].

3.1.2. Dal caso *Wirtschaftsakademie* al caso *Fashion ID*: una lettura più restrittiva della contitolarità

A un anno dal caso *Wirtschaftsakademie*, la Corte di Giustizia dell'Unione Europea è tornata a pronunciarsi su una vicenda analoga, giungendo a conclusioni non perfettamente coincidenti. Nello specifico, i giudici di Lussemburgo sono stati chiamati a valutare se Fashion ID, il gestore di una pagina web che incorporava un *social plug-in* (il pulsante "*Like*" di Facebook), dovesse essere considerato un *data controller* insieme al fornitore di tale *plug-in*, Facebook Ireland[414]. Ebbene, non sorprende la conclusione della Corte secondo cui il gestore della pagina e il *social network* fossero contitolari del trattamento. Al contrario, tale affermazione appare perfettamente in linea con quanto stabilito dalla Corte nel caso *Wirtschaftsakademie*. In quell'occasione, infatti, l'avvocato generale aveva affermato che non si ravvisavano differenze sostanziali tra il caso *Wirtschaftsakademie* e il caso Fashion ID; pertanto, non occorreva tracciare una artificiosa distinzione fra i due[415]. Malgrado ciò, il secondo ha trovato una conclusione parzialmente diversa dal primo. Pronunciandosi su *Wirtschaftsakademie,* la Corte aveva rigettato la ricostruzione avanzata dall'avvocato generale, a parere del quale gli amministratori della *fan page* erano

[412]L'esclusione del trattamento dei dati anonimi dall'ambito di applicazione della normativa sulla *data protection* era stabilita dal considerando n. 26 della Direttiva 95/46 CE ed è attualmente confermata dal medesimo considerando, il n. 26, del GDPR.

[413]A favore di una conclusione antitetica per il caso *Wirtschaftsakademie,* v. G. M. Riccio, *Titolarità e contitolarità dei dati personali alla luce della decisione della Corte di giustizia sulle* fanpage *di Facebook*, in *MediaLaws*, 2018, n. 3, pp. 352 e ss.

[414]Corte di Giustizia dell'Unione Europea, 29 luglio 2019, C-40/17*, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW e V,* disponibile *online* su https://curia.europa.eu/juris/document/document.jsf;jsessionid=CE0C6EA78A43FA822FDAB77E760ED473?text=&docid=216555&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=10620378.

[415]In questa prospettiva si muovono le conclusioni dell'avvocato generale Y. Bot, presentate il 24 ottobre 2017, nella causa C-210/16, par. 69, il quale ha affermato: <<non ravviso in proposito alcuna differenza essenziale tra la situazione di un gestore di fanpage e quella del gestore di un sito web che inserisce, all'interno dello stesso, il codice di un fornitore di servizi di *web-tracking* e favorisce così, all'insaputa dell'utente, la trasmissione di dati, l'installazione di *cookie* e la raccolta di dati a beneficio del fornitore dei suddetti servizi>>.

da ritenersi titolari solo nella misura in cui esercitavano un'influenza effettiva sul *data processing*[416], sostenendo che fossero tali a prescindere da tale condizione[417]. Diversamente, nella decisione Fashion ID, la Corte ha ritenuto che il gestore avesse assunto il ruolo di titolare solo per le fasi del trattamento in cui aveva effettivamente determinato le finalità e i mezzi. Dunque, la titolarità della Fashion ID era limitata alla raccolta dei dati tramite *plug – in* e al loro successivo trasferimento a Facebook[418].

Tale conclusione, però, non ha incontrato il consenso unanime della dottrina, giacché alcuni autori hanno sostenuto che non fosse stato adeguatamente considerato il reale meccanismo del sistema *plug – in*. In particolare, lo scopo per cui Fashion ID trattava i dati, ovvero ottenere un vantaggio economico derivante dalla maggiore visibilità dei propri prodotti sul *social* ogni volta che veniva cliccato "*Like*", non poteva essere raggiunto soltanto raccogliendo i dati dei visitatori e trasmettendoli a Facebook. Invero, affinché il *plug-in* fosse correttamente visualizzato, erano necessarie ulteriori operazioni di trattamento da parte del *social network*. Secondo questo orientamento dottrinale, quindi, la Corte avrebbe dovuto riconoscere che Fashion ID aveva determinato le finalità di tutte le azioni di trattamento essenziali al buon funzionamento del *plug-in*, a prescindere dal fatto che queste fossero materialmente eseguite da Facebook[419]. Inoltre, la dottrina in esame ha contestato ai giudici di Lussemburgo di non aver accertato chi avesse definito i parametri del trattamento dei dati, aspetto rilevante per il caso *Wirtschaftsakademie*. Al suo posto, un altro criterio ha avuto un ruolo decisivo per la Corte: l'incorporazione del *plug -in* da parte di Fashion ID nella propria pagina web. Così facendo, il gestore influenzava la fase di raccolta e trasmissione dei dati, poiché, se non fosse stato per il suo contributo, tali operazioni non si sarebbero verificate. All'opposto, egli non esercitava più alcun controllo dei dati una volta che questi raggiungevano i *server* di Facebook[420].

---

[416]Cfr. conclusioni dell'avvocato generale Y. Bot, *op. ult. cit.*, par. 72.
[417]Corte di Giustizia dell'Unione Europea, 5 giugno 2018, C-210/16, cit, par. 39.
[418]Corte di Giustizia dell'Unione Europea, 29 luglio 2019, C-40/17, cit., par. 85. Per alcune significative riflessioni in merito alle conclusioni della Corte, v. G. Giannone Codiglione, *Trattamenti multipli di dati personali e parcellizzazione degli obblighi di condotta*, in *Diritto dell'Informazione e dell'Informatica*, 2019, n. 6, pp. 1276 e ss.
[419]Tra tutti, v. J. Globocnik, *On Joint Controllership for Social Plugins and Other Third-Party Content– a Case Note on the CJEU Decision in Fashion ID*, in *International Review of Intellectual Property and Competition Law*, 2019, n. 50, pp. 1037 e ss.
[420]Così J. Globocnik, *ult. op. cit.,* pp. 1038 e ss.

Dinanzi a un simile ragionamento, è stato mosso alla Corte il rilievo di aver perso di vista la motivazione che l'aveva spinta ad interpretare in modo estensivo l'espressione "*joint controller*", ossia garantire un elevato livello di tutela agli interessati. La limitazione della titolarità a specifiche fasi del trattamento, infatti, è parsa un arretramento rispetto a questo obiettivo. Più in dettaglio, si è osservato che un approccio restrittivo alla contitolarità potrebbe risultare favorevole solo per i gestori dei siti web, poiché ne escluderebbe la titolarità per quelle attività di trattamento sulle quali difficilmente esercitano un condizionamento[421]. All'opposto, per gli utenti, la mancanza di parametri chiari per comprendere quando il gestore rivesta il ruolo di titolare e quando, invece, non lo sia, comporterebbe una diminuzione di tutela. In base a tale delimitazione della titolarità, ad esempio, il visitatore che intendesse ottenere informazioni sul trattamento dei propri dati, i quali sono stati raccolti durante la consultazione della pagina web, non potrebbe rivolgersi solo al gestore del sito, ma dovrebbe richiedere informazioni anche ai fornitori del *plug-in*. Siffatta frammentazione della protezione, unita al rischio che l'utente ignori che una richiesta al gestore non includa tutti i dati raccolti sulla sua pagina, si traduce in una tutela meno efficace per l'interessato[422].

3.2. La contitolarità nei termini di servizio dei *cloud service provider*

Pur tenendo conto della limitazione introdotta da quest'ultima pronuncia, è indubbio che la Corte di Giustizia dell'Unione Europea abbia notevolmente ampliato l'interpretazione della contitolarità. Estendendo tale lettura all'ambito del *cloud computing*, potrebbe accadere che un *cloud provider*, precedentemente ritenuto un titolare autonomo, allorchè utilizzi i dati dei clienti per i propri scopi, sia più propriamente classificato come contitolare, assieme al *cloud client*[423].

---

[421]Circa i vantaggi di una simile lettura della contitolarità per i gestori dei siti web, v. G. Ziegenhorn, M. Fokken, *CGUE: ambito di responsabilità per la protezione dei dati dei gestori di siti web,* 2019, disponibile *online* su https://www.redeker.de/de/newsletter/gewerblicher-rechtsschutz-medienrecht-und-datenschutz-2-2019.

[422]Sugli effetti negativi della limitazione della contitolarità, v. L. Edwards et al., *Data subjects as data controllers: a Fashion(able) concept?*, 2019, disponibile *online* su https://discovery.ucl.ac.uk/id/eprint/10076025/1/EdwardsFinckVealeZingales.pdf, i quali ritengono che considerare due soggetti contitolari limitatamente alle fasi del trattamento in cui determinano finalità comuni sia, nella pratica, un'operazione complessa. Tale difficoltà applicativa potrebbe compromettere i livelli di protezione garantita agli interessati, specialmente quando questi ignorano di aver acconsentito al trattamento dei dati da parte di soggetti terzi rispetto al gestore, come pure gli scopi per i quali i dati saranno trattati.

[423]In questo senso, v. Cloud Security Alliance (CSA), *Code of Conduct (COC) Self-Assessment*, maggio 2019, pp. 11 e ss, disponibile *online* su https://www.anonos.com/hubfs/CSA-Code-of-

Nonostante questa eventualità, sono pochi i fornitori di servizi *cloud* che affrontano il tema della contitolarità nei loro termini di servizio. Tra questi vi è PayPal, che, tuttavia, esclude l'esistenza di un rapporto di contitolarità tra la piattaforma e l'utente che, tramite un *account* business, tratti i dati personali di un altro cliente PayPal per i propri interessi economici. Al contrario, i ToS precisano che i due soggetti agiscono come titolari autonomi, ciascuno determinando separatamente le finalità e i mezzi di trattamento[424].

Una soluzione differente è stata adottata da Facebook che, in risposta alla sentenza *Wirtschaftsakademie*, ha introdotto un ***"****Page Insights Controller Addendum",* ove vengono delineate le circostanze in cui il *social* assume la veste di contitolare, insieme ai clienti che gestiscono una pagina sulla piattaforma[425]. Eppure, non può non rilevarsi come Facebook si distingua dalla maggior parte dei fornitori *cloud*, perché combina elementi dei vari modelli IaaS, PaaS e SaaS in un unico sistema, in cui il *social* occupa un ruolo centrale nella definizione dei contenuti. D'altronde, la peculiarità della struttura è emersa anche nella pronuncia Fashion ID, in cui la Corte ha dapprima stabilito che Facebook fosse un titolare del trattamento, per poi concentrarsi sulla natura dell'utilizzatore del *plug-in*, un cloud *client*, e valutare se fosse o meno un *joint controller*. Com'è stato precedentemente sottolineato, in un tipico rapporto di *cloud computing* la situazione è opposta: il cliente è solitamente considerato il titolare, mentre il fornitore del *cloud* è il responsabile, salvo che questi non disattenda le istruzioni del cliente e diventi, a sua volta, un *controller*. Prescindendo da tale ultima ipotesi, ci si interroga sulla possibilità che il *provider* sia qualificabile come *controller* o *joint controller*. In particolare, si fa riferimento ai casi in cui il *provider* mette a disposizione del cliente i propri *hardware* e *software* come mezzi del trattamento. Se l'uso di tali strumenti da parte del *client* fosse interpretato come un allineamento di mezzi con il *provider*, i due potrebbero essere considerati contitolari, a condizione che anche le loro

Conduct-for-GDPR_V3.2_2019_05_29.pdf, ove, a titolo esemplificativo, si riporta il caso di un *cloud provider* che elabora i dati al fine di migliorare i servizi forniti al cliente.

[424]Cfr. PayPal, *PayPal User Agreement*, ottobre 2024, disponibile *online* su https://www.paypal.com/us/legalhub/paypal/useragreement-full#top.

[425]Cfr. Facebook, *Page Insights Controller Addendum,* aprile 2023, disponibile *online* su https://www.facebook.com/legal/terms/page_controller_addendum, in cui si specifica che il rapporto di contitolarità tra Facebook e gli amministratori della pagina è limitato alla <<loro aggregazione in Insights>>; infatti, nel momento in cui questi agiscono con mezzi distinti e per scopi separati, operano come titolari autonomi.

finalità siano congiunte[426]. Qualora invece, condividessero solo i mezzi del *data processing*, fornitore e cliente agirebbero come titolari autonomi.

3.3. La struttura dei contratti di *cloud computing*

Come è stato fin qui evidenziato, i ToS occupano un ruolo centrale nei contratti di *cloud computing*. Invero, queste tipologie di accordi si caratterizzano per la presenza di clausole contrattuali standard, solitamente stabilite dai fornitori del servizio che adottano un approccio <<*take it or leave it*>>[427]. Diversamente, nei rapporti B2B, si assiste ad una maggiore negoziazione delle condizioni, in quanto le parti tendono a disporre di un uguale potere contrattuale. In entrambi i casi, comunque, è possibile riscontrare quattro categorie di clausole: i *Terms of Service (*ToS*)*, il *Service Level Agreement (*SLA*)*, *l'Acceptable Use Policy* (AUP) e il *Data Processing Agreement (*DPA*)*. Partendo dai ToS, abbiamo già rimarcato una funzione di queste clausole, vale a dire definire i ruoli ricoperti dai vari soggetti coinvolti nel *cloud computing*. Più genericamente, i ToS disciplinano il rapporto tra il fornitore e l'utente del servizio, regolando gli elementi essenziali dell'accordo, compresi gli obblighi e le responsabilità delle parti[428]. A seguire, troviamo il *Service Level Agreement*, il quale è adoperato per misurare e monitorare le prestazioni del *cloud,* in base al coinvolgimento dell'utente, oppure alla sua capacità di accedere alle risorse. Infatti, perché sia considerato soddisfacente, il servizio offerto dal *provider* deve essere facilmente fruibile per il cliente, nonché continuamente aggiornato[429]. Un'altra categoria di clausole che contraddistingue i contratti di *cloud computing* è l'*Acceptable Use Policy*. Quest'ultima è rivolta agli utenti finali, in quanto elenca le condizioni per l'utilizzo dei servizi ricompresi nel contratto.

---

[426]Sulla configurabilità della contitolarità nel settore del *cloud computing*, v. C. Millard et al., *At this rate, everyone will be a [joint] controller of personal data*!, in *International Data Privacy Law*, vol. IX, 2019, n. 4, pp. 217 e ss., i quali ritengono che la *joint-controllership* sia difficilmente riscontrabile in ambito *cloud*, fatta eccezione per i *social media*.

[427]C. A. Rohrmann, J. Falci Sousa Rocha Cunha, *Some Legal Aspects of Cloud Computing Contracts*, in *Journal of International Commercial Law and Technology*, vol. X, 2015, n. 1, p. 40, i quali affermano che gran parte degli utenti si limita ad accettare i contratti di servizi informatici perché non ne comprende il contenuto, in particolare i termini tecnici legati al settore IT.

[428]Per un'analisi accurata sui ToS, v. T. A. Lipinski, *Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements*, in *International Symposium on Information Management in a Changing World*, Berlino, Springer, 2013, pp. 92 e ss.

[429]Una disamina del *Service Level Agreement,* e dei vantaggi che derivano dal suo inserimento nei contratti di *cloud*, si rinviene nella relazione tenuta da G. Justy Mirobi, L. Arockiam alla *"International Conference on Control, Instrumentation, Communication and Computational Technologies"* del 2015*,* dal titolo *"Service Level Agreement In Cloud Computing. An Overview"*, pp. 753 e ss., disponibile *online* su https://ieeexplore.ieee.org/document/7475380.

Nello specifico, l'AUP vieta una serie di attività che i *provider* considerano inappropriate. D'altronde, l'obiettivo ultimo della *Policy* è proteggere il fornitore dalle responsabilità che possono derivare dai comportamenti scorretti degli utilizzatori. A tal scopo, ogni cliente è tenuto ad accettare l'AUP, che costituisce parte integrante dell'accordo con il *provider*[430]. Infine, il contratto include un *Data Processing Agreement*, il quale regola il trattamento dei dati effettuato nell'ambito del servizio di *cloud computing*[431].

3.3.1. Il *Data Processing Agreement* e il difficile adattamento al modello del *cloud computing*

Analizzando il *Data Processing Agreement*, si evince come il modello di cui al GDPR non sia perfettamente compatibile con il *cloud computing*. Per giungere a tale conclusione, è sufficiente considerare il primo elemento che, ai sensi del Regolamento, dovrebbe contrassegnare il DPA, giacché quest'ultimo dovrebbe imporre al *processor* di trattare i dati secondo le istruzioni del *controller (*art. 28, par. 3, lett. a, GDPR*).* Nel *cloud,* però, un requisito del genere perde ogni ragion d'essere; difatti, i clienti caricano, modificano ed eliminano i dati autonomamente, senza dipendere dal fornitore-*processor* per il trattamento attivo degli stessi. Un simile obbligo, quindi, appare sensato nei modelli di IT *outsourcing* tradizionali, dove il responsabile elabora attivamente i dati per conto del titolare, ma non nel *cloud computing*. Lo stesso vale per un'altra previsione che dovrebbe ricorrere nel DPA, cioè l'obbligo per i responsabili di adottare misure di sicurezza adeguate (art. 28, par. 3, lett. c, GDPR). Infatti, come osservato in precedenza, nel contesto del *cloud computing* il ruolo di *controller* è assunto dai clienti, i quali, avendo una conoscenza approfondita dei loro dati, sono anche i più adatti a stabilire le misure per la loro salvaguardia (ad es. crittografia, backup o altre ancora). Al contrario, i *cloud provider* hanno una pluralità di clienti, il che rende impossibile personalizzare le misure di sicurezza per ognuno. Un'altra caratteristica del DPA che mal si adatta al *cloud* è che questo dovrebbe prescrivere di conformarsi alle condizioni del GDPR

[430]Circa l'*Acceptable Use Policy (AUP)* e la sua formulazione, v. United Nations Commission on International Trade Law (UNCITRAL*), Notes on the Main Issues of Cloud Computing Contracts,* cit., pp. 15 e ss.
[431]In generale, sui tratti distintivi dei contratti di *cloud computing*, v. L. Valle et al., *Struttura dei contratti e trattamento dei dati personali nei servizi di* cloud computing *alla luce del nuovo Reg. 2016/679 UE*, in *Contratto e Impresa – Europa*, 2018, n. 1, pp. 347 e ss.

per nominare un *sub-processor* (art. 28, par. 3, lett. d, GDPR). Secondo questa disposizione, il responsabile dovrebbe ottenere il consenso preventivo del titolare prima di coinvolgere un sub-responsabile. Inoltre, il *processor* dovrebbe vincolare il *sub-processor* ai medesimi obblighi contrattuali cui è tenuto nei confronti del *controller.* In proposito, emergono due criticità: i fornitori offrono servizi basati su sub-fornitori preesistenti[432], ragion per cui i clienti possono solo scegliere se accettare i *sub-processor*, o non usufruire della prestazione. Un singolo servizio può coinvolgere centinaia di sub-responsabili, rendendo la conformità agli obblighi del titolare inattuabile[433].

Accanto a questi profili, non può non menzionarsi un altro aspetto che andrebbe necessariamente regolato nel *Data Processing Agreement*, ovvero la responsabilità per trattamento illecito dei dati. Si è già evidenziato che il legislatore europeo ha introdotto un duplice sistema di responsabilità, in virtù del quale il *controller* risponde del pregiudizio derivante dall'inosservanza del GDPR, mentre il *processor* è chiamato a rispondere qualora non adempia agli obblighi impostigli dal Regolamento, oppure quando disattenda le istruzioni del titolare. Benché sia stata formalmente ampliata la platea dei responsabili, nei rapporti B2B i fornitori tentano di escludere la loro responsabilità ogniqualvolta si verifichi un'interruzione o una discontinuità del servizio tale da provocare una dispersione, o addirittura una perdita, dei dati degli interessati[434]. A tal fine, i *provider* inseriscono nel DPA le cd. clausole di manleva, dirette a <<rivers[are] su terzi le conseguenze di tale responsabilità>>[435]. Quest'ultima viene fatta ricadere sul cliente, a sua volta professionista, il quale si impegna a manlevare il fornitore da ipotetiche pretese risarcitorie che siano avanzate nei suoi confronti. Seppur legittimo, l'uso di tali clausole da parte dei *cloud provider* si sta trasformando in un abuso, dal momento

[432]A titolo meramente esemplificativo, si può citare il caso di Dropbox che utilizza l'IaaS di Amazon per il proprio SaaS di archiviazione. In proposito, v. *Dropbox risparmia milioni di dollari creando uno storage di metadati scalabile su Amazon DynamoDB e Amazon S3*, 2020, disponibile *online* su https://aws.amazon.com/it/solutions/case-studies/dropbox-dynamodb-case-study/.

[433]Sull'inapplicabilità del modello di *Data Processing Agreement* elaborato dal legislatore europeo al *cloud*, v. W. Kuan Hon, *GDPR: Killing cloud quickly?,* marzo 2016, disponibile *online* su https://iapp.org/news/a/gdpr-killing-cloud-quickly, la quale, più in generale, afferma che <<*the GDPR would significantly complicate all modern outsourcing arrangements, not just cloud; cloud is just the prime example*>>.

[434]Sul punto, cfr. P. Sammarco, *I nuovi contratti dell'informatica. Sistema e prassi*, in F. Galgano (a cura di), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, Cedam, 2006, pp. 403 e ss.

[435] F. Benatti, *Clausole di manleva*, in P. Cendon (a cura di), *Trattato di diritto civile*, Milano, Giuffrè, 2015, p. 291. A tal riguardo, cfr. anche G.C. Adriano, *Patti di manleva e circolazione del costo del danno*, Padova, Cedam, 2012, pp. 88 e ss.

che queste assumono dei contorni sempre più estesi, ricomprendendo eventi dannosi facilmente evitabili dal fornitore, e per i quali, tuttavia, egli pretende di essere indennizzato[436].

4. Responsabilità e allocazione dei costi nel *Data Processing Agreement*

Il *cloud computing* rappresenta un valido esempio di contesto in cui il DPA viene stipulato tra parti con un potere contrattuale diseguale. Quando i titolari concludono accordi con grandi fornitori di servizi tecnologici, questi ultimi tendono ad adottare termini e condizioni standard, pensati per tutelare i loro interessi nel ruolo di *processor*. Essendo tali clausole a vantaggio dei fornitori, è molto difficile per i titolari ottenere una loro rinegoziazione. Tra gli aspetti più complessi su cui contrattare, vi è certamente la responsabilità per trattamento illecito dei dati. Com'è stato ampiamente osservato, l'art. 82 GDPR consente agli interessati di richiedere un risarcimento per i danni materiali o immateriali che derivino dal trattamento illecito dei loro dati. Se tale violazione dei dati avviene a causa di un trattamento illecito da parte di un *provider*, e se anche il *controller* è responsabile dell'accaduto, questi sono solidalmente responsabili per il pregiudizio arrecato. Se questo è vero, è altresì vero che molti fornitori cercano di limitare la propria responsabilità, fissando un tetto massimo pari all'ammontare delle commissioni pagate dal titolare-*outsourcer* nei dodici mesi precedenti[437]. Tuttavia, tale limitazione è spesso insufficiente per i titolari, i quali, in caso di violazione dei dati personali, potrebbero dover affrontare costi significativi, tra cui multe amministrative imposte dalle autorità di controllo, costi per la partecipazione alle indagini avviate dalle suddette autorità, ed ancora spese di notifica agli interessati coinvolti nella violazione.

---

[436]Sulle temibili conseguenze delle clausole di manleva nei contratti di *cloud computing*, v. N. Busca, Cloud computing *e tutela della privacy nei rapporti commerciali B2B*, in *Studium Iuris*, 2020, n. 11, pp. 1327 e ss.

[437]Cfr. Technology and Construction Court (TCC*),* 17 maggio 2024, n. HT-2020-000448*,* disponibile *online* su https://www.bailii.org/ew/cases/EWHC/TCC/2024/1185.html, dove la corte inglese, chiamata a pronunciarsi sull'inadempimento di un contratto di trasformazione digitale dei servizi di un ente pubblico, ha analizzato la legittimità della clausola di limitazione della responsabilità contenuta nell'accordo. In particolare, tale clausola prevedeva che la responsabilità complessiva del fornitore di servizi in relazione a tutte le richieste di risarcimento, perdite o danni, non potesse superare l'importo di dieci mila sterline; o comunque, un importo equivalente al 100% degli oneri versati in ottemperanza al contratto durante i dodici mesi precedenti la data dell'evento dannoso. Per un commento a tale pronuncia, v. C. Ripley, *The importance of appropriate liability caps,* maggio 2024, disponibile *online* su https://www.fsp-law.com/the-importance-of-appropriate-liability-caps/.

Inoltre, i *controller* che siano chiamati a rispondere del danno potrebbero dover sostenere spese legali, nonché dover soddisfare la pretesa risarcitoria degli interessati. Da ultimo, essi potrebbero incorrere in danni reputazionali derivanti dal trattamento illecito, che renderebbero necessario adottare misure volte a mitigarne gli effetti compromettenti[438].

Questi sono solo alcuni dei pregiudizi che un *controller* potrebbe subire a seguito di una violazione dei dati. Dinnanzi a tale vastità, i *processor* tentano di limitare la propria responsabilità, al fine di ridurre anche le spese a loro carico. La legittimità di una simile pratica, però, è ancora molto incerta, dal momento che non esiste un'interpretazione univoca dell'art. 82 GDPR. Secondo un primo orientamento, la norma potrebbe essere letta nel senso che i titolari e i responsabili sono pienamente responsabili del danno cagionato nel corso dell'attività di trattamento. Seguendo questa interpretazione, una clausola di limitazione della responsabilità non sarebbe ammissibile. A favore di tale ragionamento, viene posto l'uso ripetuto del termine <<s*hall*>>[439] nella versione inglese del Regolamento. Alla luce dei principi di interpretazione normativa, tale termine indica una disposizione obbligatoria a cui i soggetti devono conformarsi. Del resto, è un principio giuridico di base che le parti non possano escludere contrattualmente l'applicazione di una disposizione obbligatoria. Pertanto, se una norma impone un determinato obbligo, i contraenti non possano accordarsi per derogarlo. In conclusione, secondo quest'orientamento, gli attori del trattamento non possono inserire clausole che mirino a limitare la propria responsabilità. Eppure, l'art. 82 GDPR potrebbe essere letto anche in modo da consentire un contenimento della responsabilità. Per giungere a tale conclusione, occorre considerare il quarto paragrafo dell'articolo, il quale affronterebbe solo il tema della responsabilità del *controller* e del *processor* per il danno subito dall'interessato. Ciò trasparirebbe dall'utilizzo dell'espressione <<risarcimento effettivo>>[440], la quale suggerirebbe

---

[438]Così J. O'Brien, *GDPR series: Outsourcing contracts, all changed, changed utterly?,* in *Privacy e Data Protection,* vol. XVIII, 2018, n. 4, pp. 4 e ss.

[439]Ai sensi dell' art. 82, par. 2, GDPR <<*any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller*>>. Parimenti, il par. 3 dell'articolo stabilisce che <<*a controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage*>>.

[440] Ai sensi dell'art. 82, par. 4, GDPR <<qualora […] il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano […] responsabili dell'eventuale danno

che l'attenzione dell'art. 82 GDPR sia rivolta esclusivamente alla compensazione del *data subject.* D'altronde, per la regola di interpretazione normativa "*expressio unius est exclusio alterius"*, il fatto che l'articolo disciplini espressamente il risarcimento del soggetto interessato, ma ometta qualsiasi riferimento alla responsabilità tra il *controller* e il *processor*, dovrebbe essere inteso come un'esclusione intenzionale da parte del legislatore. Di conseguenza, la limitazione della responsabilità tra titolari e responsabili del trattamento apparirebbe lecita[441].

Al di là della responsabilità, un altro punto critico è l'allocazione generale dei costi. Infatti, il GDPR non specifica chi, fra il titolare e il responsabile, debba sostenere i costi legati alla conformità normativa, aspetto che viene rimesso alla negoziazione tra le parti. Se i costi derivano da una azione o omissione del fornitore di servizi, questi dovrebbe coprire le spese relative all'osservanza della normativa sulla *data protection*, oltre che dei provvedimenti delle autorità di controllo. A ciò, si aggiungono i costi di tutte le azioni necessarie a sanare la lesione causata all'interessato, come pure quelle di notifica nei suoi confronti. D'altro canto, sebbene il Regolamento, all'art. 28, par, 3, lett. h, imponga al responsabile di intervenire nei processi di audit che coinvolgono il titolare, è sempre più comune che sia quest'ultimo a dover sostenere le spese relative a tali verifiche. In un contesto del genere, in cui aspetti fondamentali come la responsabilità e la ripartizione dei costi sono rimessi alla negoziazione delle parti, un ruolo chiave potrebbe essere assunto dalle assicurazioni sulla *cybersecurity*[442]. Tramite questi strumenti, i titolari possono individuare più agevolmente le ipotesi in cui sono tenuti a rispondere dei danni e, soprattutto, stimare con maggior precisione le spese che, in seguito a un trattamento illecito, gravano su di loro. Tuttavia, per sfruttare a pieno queste assicurazioni, i *controller* devono preliminarmente verificare che le polizze coprano sia la mancata conformità alla disciplina sulla protezione dei dati, sia le

causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato>>.

[441]Sui diversi orientamenti dottrinali inerenti la limitazione della responsabilità, v. le considerazioni di E. Salami, *Examining the legality of limitation of liability clauses under the GDPR*, in *Computer and Telecommunications Law Review*, vol. XXIV, 2018, n. 8, pp. 175 e ss., che sostiene la legittimità di tali clausole.

[442]La letteratura in materia di assicurazione sulla *cybersecurity* è copiosa: A. Marotta et al., *Cyber - insurance survey*, in *Computer Science Review*, 2017, n. 24, pp. 35 e ss.; R. Adriko, J. R.C. Nurse, *Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review*, in *Information and Computer Security*, 2024, n. 5, pp. 691 e ss.; P. H. Meland et al., *Facing Uncertainty in Cyber Insurance Policies,* in F. Martinelli, R. Rios (a cura di), *Security and Trust Management,* Berlino, Springer, 2024.

violazioni dei dati personali. Inoltre, essi devono assicurarsi che i fornitori dispongano, a loro volta, di una copertura assicurativa sufficiente per far fronte agli obblighi assunti in sede negoziale. Solo così, le assicurazioni sulla *cybersecurity* possono rappresentare una valida misura a sostegno del contraente debole[443].

[443]A favore dell'assicurazione sulla *cybersecurity* come mezzo per equilibrare il rapporto tra *controller* e *processor*, v. J. O'Brien, *GDPR series: Outsourcing contracts, all changed, changed utterly?,* cit., pp. 5 e ss.

Capitolo IV

La tutela dei dati personali in Croazia fra Direttiva 95/46 CE e GDPR. Un'analisi sulla regolazione del *Data Processing Agreement*

Sommario: 1. La Direttiva 95/46 CE e la legge "ZZOP" del 2003; 2. La Croazia si conforma al GDPR: la "*Zakon o provedbi Opće uredbe o zastiti podataka*"; 2.1. L'adeguamento al GDPR, una sfida per le piccole e medie imprese croate; 3. Il *Data Processing Agreement* e il modello elaborato dall'AZOP; 3.1. La responsabilità di *controller* e *processor*: modelli a confronto; 4. La responsabilità per illecito trattamento dei dati personali. Uno sguardo alla disciplina croata

1. La Direttiva 95/46 CE e la legge "ZZOP" del 2003

In Croazia, il diritto alla protezione dei dati personali ha trovato fondamento costituzionale ancor prima che il Paese divenisse uno Stato sovrano. Difatti, questo è stato esplicitamente riconosciuto all'art. 37[444] della cosiddetta "Costituzione di Natale", adottata il 22 dicembre 1990, mentre la Croazia ha dichiarato la sua indipendenza dalla Jugoslavia l'8 ottobre 1991, quasi un anno dopo l'entrata in vigore della Costituzione. Le ragioni di un simile sfasamento temporale sono da ricondursi alle influenze giuridiche provenienti dall'Europa occidentale. Del resto, negli ultimi giorni di divisione del continente europeo in Est ed Ovest, i padri costituenti erano già a conoscenza del novero di diritti fondamentali affermatosi nei Paesi occidentali, i quali avevano adottato la Convenzione del Consiglio d'Europa sulla protezione dei dati personali solo un decennio prima, nel 1981.

Per quel che concerne la tutela dei dati personali, la Costituzione croata prevedeva il ricorso ad una legislazione secondaria che disciplinasse la materia in modo più dettagliato; tuttavia, ciò era avvenuto solo nel 2003, anno in cui la Croazia aveva adottato la legge sulla protezione dei dati personali (*Zakon o zaštiti osobnih podatak* o ZZOP)[445]. Sulla base della ZZOP, erano stati poi adottati due decreti da

[444]L'art. 37 della Costituzione croata dispone che sia garantita a tutti la sicurezza e la riservatezza dei dati personali. Inoltre, esso prevede che, in assenza del consenso dell'interessato, i dati personali siano raccolti, elaborati e utilizzati solo secondo le condizioni di legge. Ancora, l'articolo vieta l'utilizzo dei dati personali in contrasto con le finalità per cui essi sono stati raccolti.

[445]La *Zakon o zaštiti osobnih podataka*, o ZZOP, è stata adottata dal Parlamento croato il 12 giugno 2003 ed è stata pubblicata sulla Gazzetta Ufficiale "*Narodne novine*" n. 103/03. In seguito, il testo della ZZOP ha subito diverse modifiche, in particolare negli anni 2006, 2008, 2011 e 2012.

parte del Governo: il decreto sulle modalità di tenuta e registrazione dei dati personali[446]; il decreto sulle modalità di archiviazione e sulle misure tecniche di sicurezza per categorie speciali di dati personali[447]. Rispetto ai suddetti atti normativi, la ZZOP era connotata da una natura generale, in quanto regolava la gestione dei dati personali indipendentemente dal tipo di trattamento e dalla categoria di dati coinvolti; in tal modo, essa si allineava alla Convenzione 108 che era stata ratificata dalla Croazia nel 2005[448].

Passando al contenuto della legge sulla protezione dei dati personali, emerge come ad essa siano attribuibili due meriti, ovvero l'istituzione di un'autorità indipendente per la protezione dei dati (*Agencija za zastitu osobnih podataka* o AZOP), nonché aver previsto requisiti comuni alla Direttiva 95/46 CE, ancora prima che la Croazia aderisse all'Unione Europea. Infatti, malgrado l'avvicinamento in ambito giuridico, il Paese ha fatto il suo ingresso nell'Unione solo il 1° luglio del 2013. A quel punto, la ZZOP ha fedelmente recepito le disposizioni della Direttiva, senza però mancare di includere dei particolarismi nazionali. Tra questi, non possono non essere citati i quattro più rilevanti: il primo, è aver imposto a gran parte dei *data controller* l'obbligo di trasmettere i propri registri di attività di trattamento all'AZOP, così che questa potesse inserirli nel registro centrale nazionale (art. 16)[449]; il secondo, è aver onerato i titolari con più di venti dipendenti di incaricare un responsabile per la protezione dei dati personali (art. 18 bis, comma 2); il terzo, come anticipato, è aver istituto l'autorità nazionale per la protezione dei dati personali, ossia un' autorità pubblica di vigilanza (art. 27);

---

[446]Il decreto sulle modalità di tenuta e registrazione dei dati personali, *Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka*, (Gazzetta ufficiale "*Narodne novine*" n. 103/2003) prescriveva le modalità di tenuta dei registri dei dati personali a cui dovevano conformarsi tutti gli enti statali, locali e regionali, nonché le persone fisiche e giuridiche, che trattavano dati personali.

[447]Il decreto sulle modalità di archiviazione e sulle misure tecniche di sicurezza per categorie speciali di dati personali, *Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih ka tegorija osobnih podataka*, (Gazzetta ufficiale "*Narodne novine*" n. 139/04) fissava i requisiti per la conservazione, la salvaguardia ed il trasferimento di categorie particolari di dati personali. Esso prevedeva anche misure per la verifica del corretto funzionamento dei sistemi informatici e di telecomunicazione, oltre che dei *software* per la gestione di categorie particolari di dati personali.

[448]La legge di ratifica della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (*Zakon o potvrđivanju konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju*) è stata adottata dal Parlamento croato il 14 aprile 2005 ed è stata pubblicata sulla Gazzetta ufficiale "*Narodne novine - međunarodni ugovori*" n. 4/05.

[449]L'art. 16 della ZZOP sollevava dall'obbligo di trasferimento dei registri: i titolari del trattamento con un numero di dipendenti pari o inferiore a cinque; i titolari che avessero nominato un responsabile per la protezione dei dati personali. In entrambi i casi, l'esenzione era valida fintanto che i dati non fossero stati trasferiti al di fuori della Croazia.

l'ultimo, è aver riconosciuto all'AZOP un potere sanzionatorio (art. 36), che però, per motivi di cui si dirà meglio in seguito, è apparso sin da subito molto debole[450].

In relazione ad altri aspetti, invece, il contenuto della ZZOP coincideva perfettamente con il testo della Direttiva. Esemplificativo, in tal senso, era l'art. 2, comma 1, il quale enunciava la nozione di dato personale, descrivendolo come qualsiasi informazione relativa a una persona fisica identificata o identificabile, ovvero una persona la cui identità poteva essere determinata, direttamente o indirettamente, sulla base di uno o più elementi specifici della sua identità fisica, psicologica, mentale, economica, culturale o sociale; ebbene, la norma non faceva altro che ribadire la definizione di dato personale di cui all'art. 2, lett. a, della Direttiva[451].

Inoltre, al pari della normativa europea, la ZZOP ammetteva che il titolare, mediante un contratto, affidasse la gestione dei dati ad una persona fisica o giuridica che agisse per suo conto, il responsabile del trattamento. Rispetto alla Direttiva, però, la legge croata non solo richiedeva che il *processor* garantisse l'attuazione delle misure di sicurezza necessarie al trattamento; bensì, che fosse iscritto al registro dei soggetti idonei a ricoprire il ruolo di responsabile (art. 10, comma 2).

Quanto al contratto fra titolare e responsabile, la ZZOP dava delle indicazioni, seppur minime, in merito al contenuto, affermando che questo dovesse regolare i diritti e gli obblighi reciproci del *controller* e del *processor*. Nello specifico, l'atto doveva vincolare il responsabile, in primo luogo, a svolgere le operazioni sulla base delle istruzioni del titolare; in secondo luogo, a non fornire i dati personali a terzi, né a trattarli per finalità diverse da quelle concordate; infine, a garantire l'implementazione di adeguate misure tecniche e organizzative per la protezione dei dati personali, in conformità con le disposizioni della ZZOP. Ancora, la legge precisava che il contratto dovesse avere necessariamente forma scritta[452]. Dagli elementi appena descritti, si ricava come la legge croata, dal punto di vista sostanziale, ricalcasse quasi integralmente la Direttiva, mentre, dal punto di vista

[450]Per un'analisi approfondita della legge croata sulla protezione dei dati personali, v. J. Sajfert, *Croatia: Minimum Service for the Implementation, Big Service to the Public Sector*, in *European Data Protection Law Review*, vol. VI, 2020, n. 2, pp. 281 e ss.
[451]Per un parallelismo fra le disposizioni della ZZOP e quelle della Direttiva 95/46 CE, v. J. Čizmić, M. Boban, *Učinak nove EU eredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj*, in *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. XXXIX, 2018, n.1, pp. 382 e ss.
[452]Ai sensi dell'art. 10, comma 5, della ZZOP.

formale, se ne discostasse, poiché non prevedeva una forma scritta *ad probationem*[453], ma *ad substantiam.*

Anche aver istituito l'autorità per la protezione dei dati rendeva la ZZOP conforme alla Direttiva, in particolare all'art. 28, il quale invitava gli Stati Membri a nominare autorità pubbliche di controllo <<pienamente indipendenti nell'esercizio delle funzioni loro attribuite>>. Tale era l'AZOP, un'autorità di vigilanza indipendente chiamata a far rispettare le norme in materia di *data protection* e a reprimerne eventuali violazioni, sia di propria iniziativa, che su richiesta degli interessati. Affinché ciò fosse possibile, la ZZOP attribuiva all'autorità nazionale un ampio potere decisorio; infatti, qualora avesse rilevato una scorretta gestione dei dati, tanto da parte del *controller,* quanto da parte del *processor,* l'AZOP poteva disporne la regolarizzazione entro un termine stabilito. Tuttavia, questi non erano i soli provvedimenti di competenza dell'Agenzia (come pure verrà indicata l'AZOP d'ora in avanti): alcuni, precludevano del tutto la prosecuzione del trattamento in violazione della ZZOP; altri, imponevano la cancellazione dei dati personali che fossero raccolti senza una base legale; altri ancora, impedivano i trasferimenti illeciti di dati personali verso Stati terzi, o comunque verso soggetti non autorizzati a disporne. Per quanto riguarda il responsabile del trattamento, l'AZOP poteva vietarne l'operato per conto del titolare allorché questo avvenisse in contrasto con la Direttiva, o della legge croata sulla protezione dei dati personali.

Oltre a adottare tali misure, era facoltà dell'Agenzia avviare procedimenti penali o amministrativi presso l'autorità competente. Un'indicazione sul numero di azioni esercitate dall'AZOP, si ritrova nel rapporto annuale dell'attività dell'Agenzia; per l'anno 2012, ad esempio, l'autorità di vigilanza aveva avviato quattro procedimenti amministrativi e due procedimenti penali[454]. Con riferimento a questi ultimi, occorre rilevare come il codice penale croato consideri un reato l'uso

[453]L'art. 17, par. 4, della Direttiva 95/46 CE disponeva che: <<ai fini di conservazione delle prove, gli elementi del contratto o dell'atto giuridico relativi alla protezione dei dati […] sono stipulati per iscritto o in altra forma equivalente>>. Sulla forma *ad probationem* del contratto fra titolare e responsabile, v. G.M. Riccio*, Soggetti che effettuano il trattamento*, in S. Sica, P. Stanzione (a cura di), *La nuova disciplina della privacy: commento al D.lgs. 30 giugno 2003, n. 196,* Zanichelli, Bologna, 2004, pp.123 e ss.

[454]Agencija za zastitu osobnih podataka (AZOP), *Report on activities for 2012 - Izvjesce o radu za 2012. godinu*, giugno 2012, pp. 24 e ss., disponibile *online* su https://azop.hr/wp-content/uploads/2020/12/Izvjesce_o_radu_AZOP_za_2012.pdf.

non autorizzato dei dati personali, punibile con una pena detentiva da uno a cinque anni a seconda delle circostanze previste[455].

Benché avesse facoltà di adire l'autorità giurisdizionale, l'AZOP non era titolare di un potere sanzionatorio diretto. Quanto alle sanzioni, esse avevano tutte natura contravvenzionale, essendo prevista dalla ZZOP una multa massima di 40.000 *kune*, circa 5.300 euro, anche per le violazioni più gravi. Inoltre, sebbene la legge croata avesse introdotto le sanzioni, non stabiliva alcun criterio per la loro applicazione, neppure l'importo massimo della contravvenzione per infrazioni ripetute. Al contrario, la ZZOP si limitava a dichiarare l'applicabilità della multa pecuniaria ogniqualvolta i *controller,* i *processor* o i *data subject* avessero disatteso gli ordini dell'Agenzia. Alla luce di ciò, emerge come i poteri riconosciuti dalla ZZOP all'Agenzia fossero insufficienti ad assicurare il rispetto della legislazione vigente in materia di *data protection*[456].

2. La Croazia si conforma al GDPR: la "*Zakon o provedbi Opće uredbe o zastiti podataka"*

Venticinque anni dopo l'adozione della "Costituzione di Natale", l'Unione Europea definiva il nuovo assetto normativo sulla protezione dei dati[457], costituito dal Regolamento Generale sulla Protezione dei Dati (GDPR) e dalla Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (LED)[458]. Detto apparato legislativo veniva ufficialmente adottato il 27 aprile 2016, data che segnava l'inizio del periodo di transizione, in cui le autorità nazionali avrebbero dovuto trasporre la LED ed avrebbero altresì potuto implementare, a livello locale, il GDPR. Nel caso della Croazia, le autorità competenti optarono per ridurre al minimo la

[455]L'art. 146 del codice penale croato persegue l'utilizzo non autorizzato di dati personali, punendo chiunque raccolga o tratti dati personali altrui contrariamente alle condizioni di legge.
[456]Cfr. N. Gumzej, *Selected aspects of proposed new EU general data protection legal framework and the Croatian perspective*, in *Juridical Tribune,* vol. III, 2013, n. 2, pp. 194 e ss.
[457]Il 15 dicembre 2015 ha rappresentato un momento di svolta nella procedura avviata dalle Istituzioni Europee per riformare il sistema di protezione dei dati: è stato raggiunto l'accordo finale sul GDPR e sulla Direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie. Sul punto, cfr. Garante europeo per la protezione dei dati, *Relazione Annuale 2015 - Sintesi*, pp. 4 e ss., disponibile *online* su https://www.edps.europa.eu/sites/default/files/publication/ar2015_summary_it.pdf.
[458]La *Law Enforcement Directive (*LED) mira a garantire la protezione delle persone fisiche, regolando il trattamento dei dati personali che le autorità competenti pongono in essere per prevenire, accertare o perseguire reati, nonché per dare applicazione a sanzioni penali. Per un'analisi approfondita sulla portata della LED, v. M.R. Leiser, B.H.M Custers, *The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, in *European Data Protection Law Review*, vol. V, 2019, n. 3, pp. 367 e ss.

specificazione nazionale del GDPR; è indubbio, infatti, che lo Stato Membro più giovane dell'Unione sia stato alquanto cauto nell'adottare il proprio atto di adeguamento, la "*Zakon o provedbi Opće uredbe o zastiti podataka*" (Legge sull'attuazione del Regolamento Generale sulla Protezione dei Dati). D'altronde, ciò spiega la brevità dell'*iter* legislativo che ha caratterizzato l'atto, il quale si è svolto nei primi mesi del 2018 ed è culminato, il 27 aprile dello stesso anno, nell'adozione del testo definitivo da parte del Parlamento croato. Tuttavia, l'atto di adeguamento del GDPR è entrato in vigore solo nel maggio del 2018, contemporaneamente al Regolamento[459].

Malgrado il GDPR faccia ricorso a diverse clausole di apertura, e quindi consenta la differenziazione fra le regolazioni nazionali, l'atto di adeguamento croato presenta un numero limitato di clausole di specificazione, a testimonianza dell'approccio minimalista scelto del legislatore. Difatti, dei suoi cinquantasette articoli: trentuno, sono dedicati ad allineare l'organizzazione, i poteri (comprese le sanzioni amministrative) e le procedure dell'AZOP ai requisiti del GDPR; otto, si occupano della videosorveglianza. Le altre disposizioni, invece, designano l'organismo nazionale di accreditamento (art. 5), regolano il consenso dei minori (art. 19), specificano ulteriormente il trattamento dei dati genetici (art. 20) e biometrici (artt. 21-24), nonché il trattamento per scopi statistici (art. 33); ancora, consentono alle organizzazioni no-profit di rappresentare i *data subject* (art. 41). A differenza di altre giurisdizioni, quindi, l'atto di adeguamento al GDPR né traspone la LED, per la quale è stata adottata una legge separata[460], né tantomeno copre l'area della sicurezza nazionale e della difesa, come precisato all'art.1.

2.1. L'adeguamento al GDPR, una sfida per le piccole e medie imprese croate

Benché la Croazia si sia rapidamente conformata al Regolamento, l'adeguamento al GDPR rimane una questione critica per le piccole e medie

[459] Sull'implementazione del GDPR in Croazia, v. J. Sajfert, *Croatia: Minimum Service for the Implementation, Big Service to the Public Sector,* cit., pp. 282 e ss.

[460]La LED è stata attuata tramite la legge sulla protezione delle persone fisiche in relazione al trattamento e allo scambio di dati personali a fini di prevenzione, ricerca, accertamento o perseguimento di reati o esecuzione di sanzioni penali (*Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprečavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija*), la quale è entrata in vigore il 4 agosto 2018 ed è stata pubblicata sulla Gazzetta ufficiale "*Narodne novine*" n. 68/18.

imprese (PMI), le quali rappresentano più del 99% del tessuto imprenditoriale croato[461]. A differenza delle grandi aziende, infatti, le piccole realtà spesso mancano delle risorse umane e finanziarie necessarie per conformarsi alla normativa vigente in materia di protezione dei dati. Ciò, costituisce un problema non di poco conto se si considera che in Croazia, come nel resto d'Europa, il gruppo più numeroso di titolari e responsabili del trattamento è identificabile proprio nelle piccole e medie imprese.

Fra le problematiche riscontrate dalle PMI, vi è il doversi confrontare con il complesso sistema normativo sulla *data protection*: non basta osservare il Regolamento, ma occorre tener conto di tutta la legislazione nazionale applicabile al Paese specifico, nonché al settore di attività. Se questo è vero, è evidente come il livello di conformità delle imprese al GDPR differisca significativamente da uno Stato all'altro; si pensi alla Germania, che, con oltre cinquant'anni di promozione della cultura della protezione dei dati, possedeva uno standard di tutela piuttosto elevato già prima del GDPR[462]. Il rispetto di tale standard ha sicuramente agevolato le imprese tedesche, le quali hanno comunque affrontato delle difficoltà per adeguarsi al Regolamento[463], ma di una portata diversa rispetto a quelle di altri Stati Membri. In Portogallo, ad esempio, una ricerca condotta fra le PMI locali ha evidenziato come gran parte degli imprenditori ignorasse di dover adottare misure di sicurezza per la salvaguardia dei dati, come pure l'obbligo di stipulare contratti con i responsabili del trattamento[464].

---

[461]Il settore delle piccole e medie imprese è quello maggiormente presente nell'economia croata (99,7%). Le PMI impiegano quasi i tre quarti (72,2%) di tutti i dipendenti delle aziende croate (così *Centar za obiteljska poduzeća i prijenos poslovanja* (CEPOR), *Small and Medium Enterprises Report Croatia – 2019*, dicembre 2019, p. 13, disponibile *online* su https://www.cepor.hr/publikacijepolicy-dokumentiprezentacije/izvjesce-o-malim-i-srednjim-poduzecima/.

[462]Sulla tutela del diritto alla protezione dei dati in Germania, v. A.M. Zell, *Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field German Law*, in *German Law Journal*, vol. XV, 2014, n. 3, pp. 461 e ss.

[463]I problemi che le imprese tedesche hanno incontrato nell'applicare il GDPR ai loro modelli di *business* sono riconducibili a sei ordini di ragioni: la mancanza di "*know-how*", l'elevato dispendio di tempo, la complessità del linguaggio impiegato dalla normativa, gli alti costi, la formazione insufficiente e, infine, l'elevato numero di processi da adeguare. In questi termini R.C. Härting, R. Kaim, D. Ruch, *Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design*, in *Agents and Multi-Agent Systems: Technologies and Applications, 14th KES International Conference*, Berlino, Springer, 2020, p. 295.

[464]Circa gli esiti della ricerca, v. M. De Conceição Freitas, M. Mira da Silva, *GDPR Compliance in SMEs: There is much to be done*, in *Journal of Information Systems Engineering & Management*, vol. III, 2018, n. 4, pp. 4 e ss.

Per quanto riguarda la Croazia, la letteratura non forniva alcun dato sull'esperienza delle imprese nazionali; pertanto, è stato condotto uno studio su 345 PMI volto a rilevare come queste si fossero conformate al GDPR o, qualora non lo avessero fatto, cosa glie lo avesse impedito[465]. Lo studio è stato effettuato nell'ambito del progetto "*Awareness Raising Campaign for SMEs*" (ARC), il quale mira: preliminarmente, ad analizzare le problematiche riscontrate dalle PMI croate nell'adeguarsi al GDPR; successivamente, ad elaborare materiale didattico che ne agevoli il processo di "*compliance*"[466].

Passando ai risultati dello studio, questi rivelano come un numero significativo di PMI croate fatichi a raggiungere la conformità al GDPR. In particolare, solo il 37% degli imprenditori ha affermato di sentirsi adeguatamente informato sugli obblighi derivanti dal GDPR, mentre la percentuale restante ha lamentato una carenza informativa. Inoltre, è emerso come meno del 50% delle imprese coinvolte abbia attuato una politica di conservazione dei dati, pur avendo il GDPR fissato requisiti fondamentali sia sulla conservazione dei dati personali, che sulla loro cancellazione. Del resto, l'osservanza di tali requisiti è diventata ancor più cruciale a seguito alla crisi pandemica del 2020, poiché quest'ultima ha favorito l'impiego delle tecnologie da parte delle PMI, le quali hanno conseguentemente ampliato il novero dei dati oggetto del loro trattamento. Date queste circostanze, le imprese non possono esimersi dall'adottare politiche di conservazione e cancellazione dei dati, le sole ad assicurare il rispetto dei principi di minimizzazione e limitazione della conservazione dei dati. Un'altra grande sfida per le PMI croate è ottemperare al principio di trasparenza, giacché faticano ad informare i *data subject* dei trattamenti che coinvolgono i loro dati. Tra le imprese che avevano preso parte allo studio, ad esempio, solo il 50% aveva provveduto a pubblicare sul proprio sito internet *policy* in materia di privacy e *data protection*. Dalla ricerca è emerso anche un ulteriore elemento: un consistente numero di PMI ricorre a responsabili del trattamento, ma sono in poche ad aver concluso accordi per regolare il rapporto *data controller - data processor*. Sebbene, infatti, l'art. 28 del GDPR prescriva la stipula di un contratto, o di un altro atto giuridico,

[465]Lo studio è stato condotto attraverso un sondaggio anonimo distribuito tramite la piattaforma digitale "*Qualtrics*" nel periodo tra il 25 maggio 2020 e il 10 settembre 2021, in collaborazione con i partner del progetto ARC e la Camera di Commercio croata, la quale ha contattato oltre trentamila aziende affinché prendessero parte allo studio.

[466]Per un approfondimento sul progetto ARC, v. *Project ARC II – Awareness Raising Campaign for SMEs,* disponibile *online* su https://arc-rec-project.eu/about.

ogniqualvolta il trattamento dei dati sia affidato ad un *processor*, solo il 41,74% delle imprese partecipanti ha in essere accordi di questo tipo[467].

Oltre a rilevare quali fossero gli ostacoli all'attuazione del GDPR, lo studio ha evidenziato che le PMI avrebbe potuto trarre beneficio da nuove linee guida, nonché modelli, sugli aspetti più incerti del Regolamento. D'altronde, al momento della ricerca, non esistevano linee guida che adoperassero un linguaggio comprensibile ai piccoli imprenditori né in lingua croata, né tantomeno in inglese. Quanto a queste ultime, è vero che il Comitato europeo per la protezione dei dati ha pubblicato diverse linee guida rivolte ai titolari e ai responsabili del trattamento[468]; tuttavia, spesso sono troppo complesse per le PMI, le quali mancano di competenze in materia legale e IT[469]. In ragione di ciò, la Commissione Europea ha incoraggiato le autorità di protezione dei dati a fornire linee guida, modelli e strumenti digitali su misura per le esigenze specifiche delle PMI[470].

Basandosi sui risultati della ricerca, i partner del progetto ARC hanno sviluppato venti linee guida sugli argomenti che apparivano più rilevanti per le PMI croate, quali la tenuta dei registri delle attività di trattamento, il trasferimento dei dati, la valutazione di impatto e molti altri ancora[471].

3. Il *Data Processing Agreement* e il modello elaborato dall'AZOP

[467]Sui risultati dello studio condotto fra le PMI croate, v. A. Mladinić, Z. Vukić, A. Rončević, *GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises*, in *Pravni vjesnik*, vol. XXXIX, 2023, nn. 3 - 4, pp. 68 e ss.

[468]Tra tutte, v. Comitato europeo per la protezione dei dati (EDPB), *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR. Versione 2.0*, 7 luglio 2021, disponibile *online* su https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf.

[469]"IT" è l'acronimo di "*Information Technology*", espressione che si riferisce all'uso di computer e *software* per gestire informazioni. Nel contesto imprenditoriale, per competenze IT si intende la capacità di utilizzare sistemi o processi informatici che rendano più efficienti le operazioni aziendali.

[470]La Commissione Europea ha sottolineato come alcune delle autorità di protezione dei dati abbiano già sviluppato misure per aiutare le PMI a rispettare il GDPR, ad esempio <<attraverso la predisposizione di modelli per i contratti di trattamento e le registrazioni delle attività di trattamento, seminari e linee telefoniche dirette per la consultazione>>; tuttavia, <<si dovrebbero prendere in considerazione ulteriori attività destinate a facilitare l'applicazione del regolamento generale sulla protezione dei dati per le PMI>>. Così Commissione Europea, *Comunicazione al Parlamento europeo e al consiglio "La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati",* COM (2020) 264 final, 24 giugno 2020, p. 9, disponibile *online* su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020DC0264#footnote51.

[471]Fra le tematiche affrontate nelle linee guida, vi sono anche le seguenti: i principi in materia di *data protection*, le basi legali per il trattamento, le misure tecniche e organizzative per la salvaguardia dei dati, la videosorveglianza, il *marketing* diretto, la *policy s*ulla privacy, il *phishing*, i diritti degli interessati, la *data breach* e i *cookie*.

Nel contesto del progetto ARC, l'autorità croata per la protezione dei dati ha predisposto un modello di accordo sul trattamento dei dati tra titolare e responsabile del trattamento (*Data Processing Agreement* o DPA). Dal canto proprio, l'AZOP ha sottolineato più volte l'importanza di quest'atto, incentivandone l'adozione da parte di *controller* e *processor* che ne fossero privi. Esemplificativo, in tal senso, è il caso dei fornitori di servizi postali, la cui qualifica di titolare o responsabile era oggetto di dibattito. A far sorgere il dubbio, era stata la circostanza che suddetti fornitori operassero in conformità a regolamenti speciali, i quali disciplinavano tanto l'attività di consegna della posta, quanto i termini generali delle modalità di spedizione; eppure, l'Agenzia ha ritenuto che questi elementi fossero insufficienti a qualificare i fornitori come titolari del trattamento. Infatti, il *processor* resta tale anche quando agisce secondo le proprie regole, purché osservi le linee guida generali fornite dal *controller* ed in esse sia precisato lo scopo del trattamento. Al contrario, il fatto che il titolare non indichi chiaramente i mezzi del trattamento, non può far ricadere automaticamente il ruolo di *controller* in capo al *processor*; ciò, a condizione che il titolare stabilisca lo scopo del trattamento in modo così preciso, da costituire una guida per la selezione dei mezzi del trattamento. Dunque, a parere dell'Autorità croata, è possibile che lo scopo stesso costituisca un mezzo di trattamento, intendendo quest' ultimo come la misura ragionevole necessaria per raggiungere un determinato fine. Alla luce di tali considerazioni, l'AZOP ha ritenuto fondamentale per il titolare e il responsabile, ovvero il fornitore del servizio postale, concludere un contratto ai sensi dell'art. 28, par. 3, del GDPR, ove fosse chiaramente stabilito lo scopo del trattamento e, di riflesso, anche i mezzi. Inoltre, l'accordo doveva contenere informazioni in merito: all'oggetto, alla durata e alla natura del trattamento, alla tipologia di dati personali coinvolti, alle categorie di interessati, nonché ai diritti e agli obblighi del titolare. D'altra parte, l'assenza del contratto non solo induceva ad un'errata qualificazione del fornitore, ma precludeva a quest'ultimo di gestire i dati per conto del titolare, poiché è proprio l'accordo a legittimarne il trattamento (28, par. 3, GDPR)[472].

[472]Sulle figure del titolare e del responsabile del trattamento nel servizio postale, v. Agencija za zastitu osobnih podataka (AZOP), *Razgraničenje uloge voditelja obrade i izvršitelja obrade*, disponibile *online* su https://azop.hr/voditelj-i-izvrsitelj-obrade/.

Analogamente, per quanto riguarda il trattamento dei dati personali tramite sistemi di videosorveglianza, l'Agenzia ha inizialmente chiarito chi riveste il ruolo di titolare e chi quello di responsabile del trattamento: successivamente, ha ribadito l'obbligo di regolare il rapporto tra *data controller* e *data processor* attraverso un contratto o altro atto giuridico. In particolare, l'AZOP identificava: il *controller,* nella persona giuridica che utilizzava la videosorveglianza per monitorare i propri locali commerciali; il *processor*, nella società che si occupava della manutenzione del sistema di videosorveglianza per conto del titolare. Tuttavia, perché questa distinzione fosse effettivamente applicabile, le persone giuridiche addette al mantenimento degli impianti dovevano agire esclusivamente secondo le istruzioni scritte delle persone giuridiche – titolari del trattamento. Ancora una volta, il contratto appariva lo strumento imprescindibile tramite cui individuare il *controller* e il *processor*. Invero, l'accordo doveva riportare le istruzioni del titolare nei confronti del responsabile, così da chiarire quando la società di manutenzione stesse agendo nel rispetto delle prescrizioni e, quindi, stesse operando per conto del titolare in qualità di responsabile del trattamento[473].

Data la frequenza con cui veniva interrogata sulla doverosità dell'accordo fra *controller* e *processor*, come pure sulle modalità di conclusione dello stesso, e dovendo altresì considerare i risultati del progetto ARC, l'AZOP ha infine elaborato un modello di accordo sul trattamento dei dati tra titolare e responsabile ai sensi dell'art. 28, par. 3, GDPR[474].

Passando ad esaminare il contenuto di tale modello, esso stabilisce, in via preliminare, che la stipula del DPA è volta ad ottemperare all'art. 28 del Regolamento; alla luce di ciò, i termini che ricorrono nel testo vanno intesi con il medesimo significato attribuito loro dal GDPR [475].

Nel prosieguo, il modello contempla una clausola da utilizzare allorché il responsabile nomini un rappresentante all'interno dell'Unione, per poi focalizzarsi sull'oggetto del contratto. In proposito, è richiesto alle parti di

[473]Sulle figure del titolare e del responsabile del trattamento nel servizio di videosorveglianza, v. AZOP, *Uloga voditelja i izvršitelja obrade (zaposlenici voditelja obrade nisu izvršitelji obrade)*, 20 marzo 2023, disponibile *online* su https://azop.hr/uloga-voditelja-i-izvrsitelja-obrade-zaposlenici-voditelja-obrade-nisu-izvrsitelji-obrade/.

[474]AZOP, *Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3.Opće uredbe o zaštiti podataka sklapa se između,* 9 dicembre 2022, disponibile *online* su https://azop.hr/wp-content/uploads/2023/03/Ugovor-o-obradi-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-prema-clanku-28-OUZP-template.docx.

[475]AZOP, *op. ult. cit.,* par. 1.

specificare l'ambito entro il quale il responsabile fornisce servizi al titolare, così come indicato nel contratto principale. D'altronde, è solo per quanto strettamente necessario a tale attività che il titolare cede i dati al responsabile, il quale è chiamato a trattarli esclusivamente per conto del titolare e nel rispetto delle sue istruzioni. Queste ultime vanno definite all'allegato 1 dell'accordo e determinano, assieme al contratto principale, lo scopo e l'entità del trattamento dei dati. In aggiunta a quanto detto, il testo dell'AZOP incarica titolare e responsabile di definire, attraverso l'accordo, i rispettivi obblighi e diritti in conformità alla normativa sulla protezione dei dati. Suddette disposizioni sono da ritenersi prevalenti rispetto al contratto principale, il quale potrebbe disciplinare in maniera differente facoltà ed oneri delle parti. Inoltre, perché l'accordo possa dirsi rispettato, il trattamento dei dati personali deve avvenire esclusivamente sul territorio di uno Stato membro dell'Unione Europea, o di uno Stato membro dello Spazio economico europeo (SEE); pertanto, il responsabile che intenda trasferire il proprio servizio, in tutto o in parte, in un territorio extra-UE o SEE, è tenuto a concludere un accordo ulteriore con il titolare[476].

Dopo l'oggetto, il modello si dedica alle tipologie di dati trattati e alle categorie di interessati a cui questi sono riconducibili, precisando che entrambe devono essere elencate nell'allegato 1 dell'accordo; analogamente, se alcuni dei dati trattati dovessero appartenere a categorie particolari, dovrebbero essere indicati come tali all'interno del primo allegato[477].

Quanto alle istruzioni del *controller,* il modello chiarisce che, pur dovendo essere inizialmente impartite tramite DPA, queste possono successivamente essere modificate, integrate o sostituite da istruzioni individuali in forma scritta o elettronica. Difatti, il titolare ha il diritto di emettere istruzioni in qualsiasi momento, anche dopo la scadenza del contratto principale; in questo caso, però, le istruzioni devono essere considerate come una modifica di quelle iniziali. Inoltre, il DPA deve anche precisare tutti gli obblighi inerenti alle istruzioni: uno, comune ad entrambe le parti, ossia conservare le istruzioni per l'intera durata dell'accordo e per i cinque anni successivi; uno, specifico del responsabile, ovvero agire nel rispetto delle istruzioni. Benché sia gravato da tale onere, il *processor* può sospendere l'applicazione delle istruzioni quando sospetti che siano in

[476]AZOP, *op. ult. cit.,* par. 3.
[477]AZOP, *op. ult. cit.,* par. 4.

contrasto con la disciplina in materia di protezione dei dati, informando immediatamente il titolare. *A fortiori,* il responsabile può rifiutarsi di seguire le istruzioni che gli appaiono chiaramente illegali[478].

Per quel che concerne le misure di sicurezza, il testo dell'AZOP si conforma al GDPR, ponendo tale onere in capo al responsabile e chiedendogli di implementare le misure tecniche e organizzative di cui all'art. 32 del GDPR, incluse quelle previste all'allegato 2 dell'accordo. Una volta adottate, egli è libero di apportarvi delle variazioni, purché non compromettano il livello di protezione concordato con il titolare, il quale ha sempre facoltà di ottenere maggiori dettagli sulle misure di protezione in corso. Nel medesimo paragrafo delle misure di sicurezza, il modello regola anche l'eventuale nomina di un responsabile della protezione dei dati (DPO), disponendo che il *processor* fornisca i suoi dati di contatto, soprattutto se esterno, all'allegato 6 dell'accordo. Laddove sia stato indicato un DPO, e questo si assenti per un periodo prolungato, il responsabile può designare un sostituto temporaneo senza dover richiedere il consenso del titolare. Qualora, invece, la designazione del nuovo DPO sia definitiva, il *processor* deve ottenere l'approvazione del *controller*[479].

A seguire, il modello detta: da una parte, gli obblighi di cooperazione del responsabile, il quale deve supportare il titolare nell'adempimento degli obblighi legali derivanti dalle norme in materia di *data protection*, in particolare quelli previsti tra l'art. 32 e l'art. 36 del Regolamento[480]; dall'altra, gli oneri informativi che il responsabile ha nei confronti del titolare. Infatti, ogniqualvolta il *data subject* eserciti i diritti di cui agli artt. 12 – 23 GDPR[481], il *processor è* tenuto ad avvisare il *controller* entro quindici giorni lavorativi. Nello stesso termine, il responsabile deve altresì comunicare al titolare che ha ricevuto istanze degli interessati sull'azionabilità dei propri diritti, le quali avrebbero invece dovuto

[478]AZOP, *op. ult. cit.,* par. 5.
[479]AZOP, *op. ult. cit.,* par. 6.
[480]Gli artt. 32 – 36 GDPR impongono al responsabile di coadiuvare il titolare: nella valutazione dei rischi e nell'implementazione delle misure di sicurezza; nell'identificazione e nella comunicazione di eventuali violazioni dei dati personali al titolare del trattamento; nella preparazione della documentazione necessaria per le comunicazioni previste dalla normativa sulla *data protection,* in particolare quelle agli interessati; nella redazione delle valutazioni di impatto sulla protezione dei dati personali e nell'eventuale consultazione preventiva con l'autorità di controllo competente.
[481]Il Regolamento, agli artt. 12-23, riconosce all'interessato i diritti di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e, infine, opposizione al trattamento dei dati.

essere rivolte al titolare. In tal caso, il responsabile deve astenersi dal rispondere ai *data subject,* salvo diverse istruzioni del titolare[482].

Per quanto riguarda le violazioni dei dati personali, il modello va a specificare quanto disposto dall'art. 33 GDPR, ovvero che il responsabile informa il titolare di eventuali *data breach* << senza ingiustificato ritardo>>, prevedendo che il *processor* notifichi al *controller* la violazione entro ventiquattro ore dal rilevamento. Diversamente, il modello non aggiunge nulla rispetto al Regolamento circa la notifica del *data breach* all'autorità di controllo; esso si limita a ribadire che la comunicazione spetta al titolare, il quale è supportato dal responsabile sia nel reperire informazioni sulla violazione, che nell'adottare misure risolutive[483].

Come per la violazione dei dati, anche la figura del sub- responsabile del trattamento è stata regolata dall'AZOP in maniera analoga al GDPR (art. 28, parr. 2 e 4): la sua nomina è condizionata al consenso scritto del titolare; è soggetto agli stessi obblighi che gravano sul *processor* in virtù dell'accordo titolare-responsabile; ogni sua sostituzione, o aggiunta, deve essere comunicata al titolare dal responsabile. Rispetto a tali variazioni, però, il modello fa una precisazione, in quanto riconosce al titolare il diritto di opporvisi entro il termine prestabilito di dieci giorni. Non si discosta dal Regolamento, invece, per quanto attiene alla responsabilità del *sub-processor*, poiché afferma solo che a rispondere delle azioni che questi compie in violazione dell'accordo è il responsabile del trattamento[484].

Relativamente alla cessazione del DPA*,* l'Agenzia non ha solo onerato il *processor* della restituzione o cancellazione dei dati oggetto del trattamento, ma ha richiesto allo stesso una conferma scritta dell'avvenuta cancellazione. Inoltre, l'AZOP ha esteso la vigenza dell'accordo, limitatamente alle norme sulla *data protection*, sino al momento della completa eliminazione o riconsegna dei dati[485].

Infine, il modello si concentra sulla risoluzione del contratto principale, contemplando due differenti ipotesi: la risoluzione straordinaria, esercitabile dal titolare qualora il responsabile non osservi gli obblighi derivanti dal DPA, oppure violi gravemente il Regolamento, la normativa nazionale sulla protezione dei dati

[482] *Agencija za zastitu osobnih podataka* (AZOP), *op.ult.cit.,* par. 7.
[483] AZOP, *op. ult. cit.,* par. 8.
[484] AZOP, *op. ult. cit.,* par. 9.
[485] AZOP, *op. ult. cit.,* par. 10.

o le istruzioni del titolare[486]. La risoluzione ordinaria, in conseguenza della quale il responsabile è tenuto, come per la cessazione dell'accordo, a restituire o cancellare tutti i documenti, dati e supporti dati ricevuti dal titolare, a meno che la cancellazione non sia vietata dalle disposizioni nazionali o dell'Unione. Il rispetto di tale obbligo può essere verificato dal *controller* sia personalmente, che avvalendosi di esperti indipendenti non concorrenti. Questi, però, non sono gli unici oneri che derivano dalla risoluzione ordinaria, poiché il *processor,* anche dopo la conclusione del contratto principale, è obbligato a mantenere il riservo sui dati trattati[487].

Nel modello di accordo appena descritto, l'AZOP non ha omesso di regolare la responsabilità del *controller* e del *processor* nei confronti del *data subject*[488]. Tuttavia, benché l'Agenzia avesse la possibilità di specificare quanto già stabilito, in via generale, dal Regolamento, si è limitata a rinviare all'art. 82 GDPR sia per quanto riguarda la responsabilità in solido del titolare e del responsabile, sia per quel che concerne la prova liberatoria. Infatti, il modello esclude la responsabilità della parte che dimostri di non aver cagionato il danno all' interessato; in altri termini, la non imputabilità dell'evento dannoso.

Quanto alla ripartizione di responsabilità, il modello dispone che, su richiesta del titolare, il responsabile è obbligato a sollevarlo da qualsiasi pretesa risarcitoria degli interessati, a condizione che questa derivi da una violazione degli obblighi imposti al responsabile dal Regolamento, o da azioni che il responsabile compie in contrasto con le istruzioni del titolare. Il modello sembra, quindi, discostarsi dal GDPR, in quanto attribuisce al *controller* la facoltà di richiedere l'esonero dalla responsabilità; in realtà, l'AZOP non ha fatto altro che riproporre il contenuto dell'art. 82, par. 2, GDPR, il quale stabilisce che <<un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento>>. Sebbene l'AZOP abbia adottato una formulazione infelice per disciplinare la responsabilità del *processor*, poiché sembra aver rimesso la sua attribuzione all'iniziativa del *controller*, il quale può

[486] AZOP, *op. ult. cit.,* par. 12.
[487] AZOP, *op. ult. cit.,* par. 13.
[488] AZOP, *op. ult. cit.,* 11.

apparentemente beneficiare di una clausola di manleva[489]; in realtà, il modello ascrive la responsabilità al *processor* nelle medesime ipotesi del GDPR, vale a dire per inosservanza dei propri obblighi o delle istruzioni del titolare. Pertanto, è evidente che il modello non riconosce al titolare alcuna esclusione di responsabilità, essendo il responsabile l'unico a poter rispondere del danno nelle ipotesi ivi contemplate.

3.1. La responsabilità di *controller* e *processor*: modelli a confronto

Le clausole contrattuali standard della Commissione Europea e il modello AZOP di Data Processing Agreement

L'Autorità croata per la protezione dei dati ha fornito ai *controller* e ai *processor* uno strumento volto ad agevolare il loro processo di adeguamento al GDPR, in special modo all'art. 28. Ovviamente, tale intervento ha rilevanza solo a livello nazionale, per cui gli attori del trattamento che operano al di fuori della Croazia devono rifarsi ad un diverso modello di *Data Processing Agreement*: le clausole contrattuali standard della Commissione Europea. È vero, infatti, che il Regolamento impone a titolari e responsabili di concludere un accordo per il trattamento dei dati, ma riconosce anche alle autorità di controllo, nonché alla Commissione Europea, il potere di emettere clausole contrattuali standard da utilizzare come DPA[490].

In ragione di ciò, il 4 giugno 2021 la Commissione ha approvato il set di clausole contrattuali tipo che disciplina i rapporti tra titolari e responsabili del

[489]La manleva è la pattuizione atipica con la quale una parte (mallevadore) assume in proprio un obbligo di natura risarcitoria, facendosi carico del rischio associato al verificarsi di un evento che comporta conseguenze economiche negative per il patrimonio dell'altra parte (il manlevato). Tuttavia, si è dinnanzi ad un patto di manleva <<soltanto nell'ipotesi in cui l'evento che faccia scattare l'obbligazione del mallevadore sia estraneo alla sua sfera di controllo e di influenza, giacché qualora l'evento originatore della responsabilità del manlevato fosse sotto il controllo del mallevadore (*rectius*, quando lo stesso mallevadore fosse responsabile di tale evento), a ben guardare, l'obbligazione di manleva non costituirebbe una vera e propria garanzia, bensì` rappresenterebbe una c.d. garanzia generica, semplicemente rafforzativa della posizione giuridica originariamente assunta dall'obbligato (mallevadore)>>. Così A. Franchi, *Riflessioni sulla manleva*, in *Contratto e Impresa*, n.1, 2017, pp. 162 e 163. Su posizioni simili, v. L. Ducange, *Patto di manleva e prescrizione del diritto del manlevato* Commento a Cass., 1° dicembre 2021, n. 37709 (ord.),* in *Pactum,* n. 3, 2022, pp. 383 e ss., il quale fa coincidere l'evento provocatore del danno con un inadempimento o un fatto illecito commesso dal manlevato, o che sia comunque ad egli imputabile.

[490] L'adozione di clausole contrattuali standard da parte della Commissione Europea e delle autorità di controllo è prevista, rispettivamente, ai parr. 7 e 8 dell'art. 28 GDPR. In particolare, al settimo paragrafo si precisa che <<La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 [atto giuridico fra titolare e responsabile] e 4 [atto giuridico fra responsabile e sub-responsabile] del presente articolo e secondo la procedura d'esame di cui all'articolo 93>>.

trattamento (SCCs)[491]. Queste ultime costituiscono un modello di accordo che *controller* e *processor* possono utilizzare per conformarsi alle norme del GDPR, nello specifico a quelle sull'esternalizzazione del trattamento dei dati. Emerge così che l'adozione delle SCCs non è obbligatoria per i titolari e i responsabili, i quali dispongono di quattro diverse opzioni per stipulare il loro DPA. La prima, è ricorrere alle clausole standard nella loro interezza, potendo in tal caso considerarle come un contratto autonomo, o come un *addendum* ad un contratto più ampio, il *Master Services Agreement*. La seconda, è affiancare alle SCCs, le quali vengono integralmente riportate nel contratto, clausole o misure di sicurezza aggiuntive. La terza è adottare le clausole contrattuali tipo solo in parte, inserendone alcune in accordi già esistenti. L'ultima, è ignorare le clausole della Commissione ed elaborare dei modelli propri, purché questi includono tutte le disposizioni richieste dal GDPR.

Alla luce di tali alternative, la scelta più conveniente per le parti appare quella di includere negli accordi tutte le SCCs; difatti, solo in questo caso la presenza delle clausole è tale da assicurare il rispetto degli standard del GDPR. Al contrario, se fossero inserite solo alcune delle SCCs, queste non garantirebbero la conformità del DPA al Regolamento; lo stesso, succederebbe se fossero incluse tutte le SCCs, ma ne fosse modificato il testo. È precluso, quindi, ai titolari e ai responsabili emendare le clausole contrattuali tipo, le quali perderebbero la loro funzione di garanzia. Tuttavia, questi possono precisarne il contenuto, dando maggiori dettagli su: le modalità di esercizio del diritto di *audit*, le sedi di archiviazione dei dati, il termine entro il quale i dati devono essere restituiti al titolare alla fine del trattamento e molti altri elementi ancora. D'altronde, queste aggiunte hanno una duplice utilità: consentono al *controller* di allineare le clausole contrattuali tipo ai modelli di DPA esistenti, oppure ai suoi processi interni; permettono al *processor* di bilanciare le SCCs che appaiono più favorevoli ai titolari[492].

[491]La Commissione Europea ha adottato il set di clausole contrattuali tipo con la Decisione di esecuzione (UE) n. 915 del 2021. Tramite Decisione di esecuzione, la Commissione ha altresì introdotto clausole contrattuali standard sul trasferimento di dati personali verso paesi terzi ed organizzazioni internazionali.

[492]Sull'utilizzo delle clausole contrattuali standard della Commissione da parte degli operatori del mercato europeo, v. L. Brodahl et al., *EU Commission Publishes Template Data Processing Agreement*, giugno 2021, disponibile *online* su https://www.wsgrdataadvisor.com/2021/06/eu-commission-publishes-template-data-processing-agreement.

Fra gli aspetti che non vengono affrontati dalle clausole contrattuali standard e che, pertanto, meriterebbero un approfondimento da parte degli attori del trattamento, vi è la responsabilità dei titolari e dei responsabili. Lungi dal dedicarvi una clausola *ad hoc*, la Commissione Europea menziona la responsabilità solo una volta, all'allegato rubricato <<Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati>>[493]. Dunque, malgrado la Commissione riconosca la necessità di clausole specifiche sulla responsabilità, in quanto richiede che tutte le misure dell'allegato siano definite in modo non generico dalle parti, non fornisce loro alcun'indicazione, limitandosi a richiedere che il DPA preveda, fra le altre, <<misure per garantire la responsabilità>>.

Traspare così il limite delle clausole contrattuali standard, aver rimesso aspetti cruciali del rapporto *controller-processor* alla libera regolazione degli stessi, non in ultimo la responsabilità di cui all'art. 82 GDPR.

Ebbene, proprio in tema di responsabilità, non può non rilevarsi come il modello AZOP abbia fornito maggiori indicazioni ai titolari e i responsabili che si accingono alla stipula del *Data Processing Agreement*. Se non altro, l'accordo dell'Autorità croata non omette di considerare la responsabilità; all'opposto, gli dedica un apposito paragrafo, tracciando, pur con tutti i limiti che lo caratterizzano, delle "linea guida" per il *controller* e il *processor.*

Le clausole contrattuali standard della Datatilsynet

Nel 2018, l'Autorità danese per la protezione dei dati (*Datatilsynet*) ha rilevato quanta difficoltà avessero le aziende nazionali a concludere accordi di trattamento dei dati conformi ai requisiti minimi di cui all' art. 28 del GDPR[494]. In conseguenza di ciò, l'Autorità ha esercitato la facoltà, attribuitagli dal

[493]L'allegato <<Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati>> è il terzo della Decisione di esecuzione (UE) n. 915 del 2021.

[494]Nell'ambito del progetto finanziato dall' UE "STAR II" (*Support small and medium enterprises on the data protection reform* II**)**, sono state ricostruite le principali sfide che il GDPR ha posto alle PMI europee; in particolare, per le imprese danesi ha costituito una sfida: adottare politiche di cancellazione e conservazione, attuare pratiche di minimizzazione dei dati, nonché decidere quale fosse il livello appropriato di implementazione del Regolamento. A queste, si aggiungono le difficoltà derivanti dalla terminologia vaga e non specifica che caratterizza il GDPR. Sui risultati del progetto "STAR II" in Danimarca, v. A. Mladinić, Z. Vukić, A. Rončević, *GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises*, cit., p. 60. Più in generale, sugli obiettivi del progetto, v. L. Cochrane, L. Jasmontaite-Zaniewicz, D. Barnard-Wills, *Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises,* in *European Data Protection Law Review*, vol. VI, 2020, n. 3, pp. 353 e ss.

Regolamento, di adottare clausole contrattuali standard (SCCs) per regolare il rapporto tra *controller* e *processor*. Tale modello è stato poi sottoposto all'EDPB in osservanza degli artt. 28, par. 8, e 64, par.1, lett.d, GDPR, i quali stabiliscono che un'autorità di controllo può adottare clausole contrattuali standard in conformità del meccanismo di coerenza[495], ossia coinvolgendo l'EDPB e, ove rilevante, la Commissione Europea. Nel luglio 2019, il Comitato europeo per la protezione dei dati ha emesso un parere[496] sulle clausole contrattuali tipo dell'Autorità danese, la prima ad aver presentato delle SCCs all'EDPB. Alla luce di tale parere, la *Datatilsynet* ha aggiornato il proprio modello e lo ha nuovamente sottoposto all'EDPB, concludendo così la procedura di consultazione[497].

Come per le clausole contrattuali standard della Commissione Europea, non vi è alcun obbligo per gli attori del trattamento di utilizzare le SCCs dell'Autorità danese, a patto che i loro DPA soddisfino i requisiti del GDPR. Eppure, ricorrere alle clausole contrattuali tipo è particolarmente vantaggioso per *controller* e *processor*, poiché impedisce alla *Datatilsynet* di esaminare l'accordo nelle parti in cui riproduce le SCCs[498].

Passando al contenuto delle clausole contrattuali standard, non può non considerarsi il ruolo avuto dal Comitato europeo per la protezione dei dati, il quale ha formulato sia osservazioni generali sugli accordi di trattamento dei dati, che commenti specifici sul modello dell'Autorità danese. Esemplificativo, in tal senso, è il rilievo dell'EDPB circa le misure tecniche e organizzative che spetta adottare al *processor*; infatti, a parere del Comitato, il modello avrebbe dovuto includere una sezione in cui far definire alle parti le misure adeguate ad assistere il titolare del trattamento, nonché l'ambito e l'entità dell'assistenza richiesta. Un apposito spazio avrebbe dovuto essere dedicato anche agli altri obblighi di assistenza di cui all'art. 28, par. 3, GDPR; in particolare, quello che impone al responsabile di garantire livelli minimi di sicurezza, adottando misure che riducano il rischio per i diritti e le

---

[495]Il meccanismo di coerenza, di cui all'art. 63 GDPR, è uno strumento per la cooperazione tra le autorità di controllo e la Commissione Europea, volto ad assicurare un'applicazione uniforme del Regolamento in tutti gli Stati Membri dell'Unione Europea.

[496]Il parere n. 14 del 2019, adottato dal Comitato europeo per la protezione dei dati il 9 luglio 2019.

[497]Per approfondimenti, v. A. Fernandez, *EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28(8) GDPR*, in *European Data Protection Law Review,* n. 4, 2019, pp. 523 e ss.

[498]Cfr. *Datatilsynet*, *Standardkontraktsbestemmelser vedtaget af Datatilsynet*, dicembre 2019, disponibile *online* su https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet/.

libertà delle persone fisiche (art.28, par. 3, lett. f). Queste misure, così come le precedenti, dovrebbero essere indicate dalle parti all'allegato C dell'accordo[499].

Inoltre, l'EDPB ha domandato alla *Datatilsynet* di integrare le disposizioni relative al sub-responsabile, osservando che qualsiasi clausola conferisca l'autorizzazione al sub-trattamento, sia generale che specifica, dovrebbe essere compresa nelle SCCs, o costituire un loro allegato. Allo stesso modo, anche l'elenco dei sub-responsabili approvati dal titolare dovrebbe far parte delle clausole contrattuali standard. Il Comitato europeo ha anche espresso l'esigenza di inserire una clausola che riconosca al titolare il diritto di opporsi alla modifica dei sub-responsabili, indicando il termine entro cui esercitare tale facoltà [500].

Nonostante l'EDPB abbia formulato osservazioni su molte delle clausole dell'Autorità danese, non ha richiesto integrazioni o variazioni della clausola numero 13, la sola a menzionare la responsabilità di *controller* e *processor*. Invero, quest'ultima consente alle parti di disciplinare aspetti del trattamento che non siano stati regolati da alcuna SCCs, tra i quali anche la responsabilità. Nulla aggiunge, però, sui criteri di imputazione della responsabilità, né tantomeno sulla prova liberatoria o sull'ipotesi di responsabilità solidale che è specificatamente prevista dal Regolamento. Dinanzi all'esiguità di questa clausola, ci si sarebbe aspettati che l'Autorità danese avesse preteso maggiori precisazioni, proprio come per le misure organizzative e di sicurezza. Al contrario, l'EDPB si è limitata a raccomandare che i paragrafi aggiuntivi dell'accordo, siano essi sulla responsabilità, sulla giurisdizione o su qualunque altro termine, non contraddicano le disposizioni pertinenti del GDPR, né compromettano il livello di protezione offerto dal Regolamento o dallo stesso DPA[501].

Alla luce di tali considerazioni, emerge come il modello dell'Autorità danese abbia effettivamente avvantaggiato le imprese locali, le quali concludono accordi nel rispetto del GDPR allorché inseriscono le SCCs. Tuttavia, occorre altresì rilevare che la *Datatilsynet* ha tralasciato aspetti rilevanti del trattamento dei dati, fra i quali la responsabilità del *controller* e del *processor*. Difatti, le clausole

[499]Comitato europeo per la protezione dei dati o EDPB, *Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR*), 9 luglio 2019, par. 3.2.9, disponibile *online* su https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.
[500]EDPB, *op. ult. cit.,* par. 3.2.7.
[501]EDPB, *op. ult. cit.,* par. 3.2.13.

contrattuali standard, salvo ribadire la necessaria osservanza del GDPR, rimettono la disciplina della responsabilità interamente alle parti. In questo modo, il modello danese non fa che favorire l'inserimento di clausole peggiorative per la parte debole, come quella in cui quest'ultima si obbliga a tenere indenne l'altra parte da eventuali pretese risarcitorie.

In conclusione, è indubbio che la *Datatilsynet* debba essere considerata un modello per le altre autorità di controllo, essendo stata la prima ad attivare la procedura prevista dal Regolamento per l'elaborazione delle clausole contrattuali standard; eppure, essa ha disciplinato la responsabilità in modo meno efficace dell'Autorità di protezione croata, che si conferma l'unica ad aver dedicato un intero paragrafo del proprio DPA alla responsabilità di *controller* e *processor.*

4. La responsabilità per illecito trattamento dei dati personali. Uno sguardo alla disciplina croata

Alla luce della Direttiva 95/46 CE, colui che avesse subito un danno per l'illecito trattamento dei dati aveva diritto ad essere risarcito dal titolare; quest'ultimo, poteva essere esonerato dalla responsabilità qualora avesse provato che l'evento dannoso non gli era in alcun modo imputabile[502]. Detta disposizione poteva essere interpretata sia come responsabilità soggettiva, che come responsabilità oggettiva; in entrambi i casi, però, l'onere della prova spettava al *controller*, il quale era chiamato a dimostrare: la sua non colpevolezza, laddove la responsabilità fosse intesa come soggettiva; l'evento fortuito imprevedibile ed inevitabile che aveva causato il danno, se alla responsabilità veniva attribuita natura oggettiva. D'altronde, il legislatore europeo era ben consapevole che il concetto di colpa, il suo onere della prova, nonché la sua esenzione, erano regolati in maniera diversa a seconda dello Stato membro; pertanto, egli ha evitato di menzionarli, lasciando ai legislatori nazionali la discrezionalità di applicare, nei loro sistemi giuridici, il tipo di responsabilità più idoneo a conseguire gli obiettivi della Direttiva.

Secondo la legge croata sulla protezione dei dati personali (ZZOP), il titolare era soggetto alle disposizioni generali in materia di risarcimento del danno (art. 26, comma 2). Dunque, veniva estesa anche al *controller* l'applicazione

[502]La responsabilità del titolare del trattamento è disciplinata dall'art. 23 della Direttiva 95/46 CE.

dell'art. 1045 codice civile croato (ZOO), il quale stabilisce che chi provoca un danno è tenuto a risarcirlo, a meno che non dimostri che il danno non si è verificato per sua colpa. Essendo sussunta sotto tale norma, la responsabilità per trattamento illecito dei dati veniva a qualificarsi come soggettiva. Del resto, se il legislatore nazionale avesse voluto sottoporre il titolare ad una responsabilità oggettiva, lo avrebbe stabilito esplicitamente.

Ad ogni modo, le questioni interpretative sono state superate con l'entrata in vigore del Regolamento; infatti, essendo le sue disposizioni direttamente applicabili, il GDPR ha escluso la trasposizione delle norme nazionali sulla responsabilità al danno da trattamento illecito di dati. La qualificazione della responsabilità diventa allora una problematica residuale, limitata ai soli aspetti non regolati dal GDPR.

Diversamente, il Regolamento non è riuscito a fugare i dubbi circa la natura del danno risarcibile. In passato, la Direttiva 95/46 CE non specificava per quale tipo di pregiudizio gli interessati avessero diritto al risarcimento; in ragione di ciò, gli Stati Membri avevano adottato approcci differenti a riguardo, soprattutto rispetto alla risarcibilità del danno non patrimoniale. Ad esempio, nel Regno Unito, il danno morale da trattamento illecito di dati è stato ammesso solo nel 2015, con il caso "*Vidal-Hall* contro *Google Inc*.". In tale occasione, la Corte d'Appello di Londra ha ritenuto inaccettabile che il diritto alla protezione dei dati personali, riconosciuto come fondamentale dalla Carta di Nizza, potesse essere violato dal titolare quasi senza conseguenze, le quali si verificavano solo nei rari casi in cui l'interessato avesse subito anche una perdita economica[503].

Date le diverse posizioni assunte dagli Stati Membri, il legislatore europeo, nel GDPR, ha chiarito che a dover essere risarcito è << chiunque subisca un danno materiale o immateriale causato da una violazione del […] regolamento>>[504]. Tuttavia, cosa debba intendersi per danno non patrimoniale, e in quali circostanze esso comporti il diritto al risarcimento, è una questione tutt'altro che risolta, dal momento che, fra i vari Stati Membri, esistono differenze notevoli sul significato di danno immateriale e sulla sua risarcibilità.

[503]*Court of Appeal of London*, 27 marzo 2015, n. A2/2014/0403, disponibile *online* su https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf
[504]Ai sensi dell'art. 82, par. 1, GDPR.

In Croazia, il codice civile fa riferimento a un concetto generale di danno, il quale include sia il pregiudizio patrimoniale, che quello non patrimoniale[505]; dunque, non vi è mai stato alcun dubbio che si potesse rispondere per il danno non patrimoniale causato dalla violazione del diritto alla protezione dei dati personali. All'opposto, le pronunce giurisprudenziali in materia di responsabilità da trattamento illecito dei dati ne hanno confermato la risarcibilità, talvolta arrivando a riconoscere il danno immateriale come l'unico pregiudizio esistente. Ciò, è proprio quanto stabilito dalla Corte distrettuale di Zagabria (*Županijski sud u Zagrebu*) in un caso del 2017, ove la ricorrente lamentava che le proprie generalità fossero state utilizzate, senza il suo consenso, in una campagna promozionale. Ebbene, la Corte ha assegnato alla parte istante un'equa compensazione per la violazione dei diritti della personalità (di cui si dirà meglio più avanti): ossia, per il solo danno non patrimoniale[506].

Posto che la violazione dei dati personali è in grado di determinare un pregiudizio diverso da quello materiale, ci si è chiesti se questo costituisca una forma autonoma di danno non patrimoniale. Un simile interrogativo sorge dalla circostanza che, nell'ordinamento croato, queste tipologie di danni sono tendenzialmente ricondotte alla violazione dei diritti della personalità. Tali diritti sono elencati, in maniera non esaustiva, all'art. 19, co. 2, del codice civile, il quale annovera nella categoria: il diritto alla vita, alla salute fisica e mentale, alla reputazione, all'onore, al rispetto, al nome, alla privacy sulla propria vita personale e familiare e, infine, alla libertà. Sebbene quelli inclusi nel codice civile siano i diritti della personalità violati più comunemente, nulla impedisce alle corti di riconoscerne altri.

Quanto al danno derivante dalla violazione dei dati personali, esso può certamente essere ricondotto all'inosservanza di uno dei diritti della personalità. Tuttavia, appare altresì ipotizzabile che il diritto alla protezione dei dati, in quanto fondamentale, costituisca un diritto della personalità autonomo, dalla cui violazione derivi un danno immateriale a sé stante. Rispetto a tale illazione, la dottrina maggioritaria osserva che non vi è alcun bisogno di individuare un nuovo diritto

[505]L'art.1046 del codice civile croato, o ZOO, definisce il danno come una perdita patrimoniale (perdita economica pura), un mancato incremento patrimoniale (perdita di profitto) o una violazione dei diritti della personalità (danno morale).
[506]*Županijski sud u Zagrebu*, 28 marzo 2017, Gžn -748/13-7, disponibile *online* su https://www.iusinfo.hr/sudska-praksa/ZSRH201374B8A7.

della personalità, poiché le conseguenze della violazione dei dati personali sono già contemplate nella violazione di altri diritti della personalità. Di norma, infatti, il danno non patrimoniale da illecito trattamento dei dati si manifesta come violazioni del diritto alla privacy sulla vita personale e familiare, o comunque di altri diritti della personalità[507].

Sulla base di tali argomentazioni, non può non rilevarsi come il Regolamento abbia posto fine a due grandi questioni: la qualificazione della responsabilità per trattamento illecito dei dati; la risarcibilità del danno non patrimoniale da violazione del diritto alla protezione dei dati personali. D'altra parte, non può negarsi che il GDPR abbia dato vita ad altre problematiche; ad esempio, quelle sul *Data Processing Agreement*, alla cui risoluzione sono state chiamate la Commissione Europea e le autorità di controllo nazionali. Tuttavia, quanto realizzato finora dalla Commissione, così come dalle singole autorità nazionali, appare insufficiente a garantire la diffusione di *Data Processing Agreement* che tutelino realmente le parti coinvolte. Perché ciò avvenga, occorre che siano formulate delle nuove clausole contrattuali standard da parte della Commissione Europea, o comunque da un numero significato di autorità di controllo nazionali, le quali facciano maggiore chiarezza sugli aspetti più oscuri del Regolamento, primo fra tutti quello della responsabilità *ex* art. 82 GDPR.

[507]Per tutti, v. M. Bukovac Puvača, A. Demark, *Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede*, in *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. XL, 2019, n. 1, pp. 287 e ss.

Bibliografia

ACCIS, *Position Paper on the Consultation on the legal framework for the fundamental right to protection of personal data,* dicembre 2009, pp. 3 e ss, disponibile *online* su: https://homeaffairs.ec.europa.eu/document/download/7d7387285a7d4b61b2329aa3a1747152_en?filename=accis_en.pdf&prefLang=cs.

ADRIANO G.C., *Patti di manleva e circolazione del costo del danno*, Padova, Cedam, 2012, pp. 88 e ss.

ADRIKO R., NURSE J. R.C., *Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review*, in *Information and Computer Security*, 2024, n. 5, pp. 691 e ss.

ALBANESE F., CARDINALI I., *Il principio di responsabilizzazione (*accountability*),* in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance, vol. I, Pisa, Pacini Giuridica, 2023, pp. 507 e ss.

ALDHOUSE F.G.B., *U.K. Data Protection – Where are we in 1991?*, in *Yearbook of Law Computers and Technology*, 1991, n. 5, pp. 180 e ss.

AVITABILE A., *Il* Data Protection Officer, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, Zanichelli, 2017, pp. 331 e ss.

BAMBERGER K. A., MULLIGAN D. K., *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, in *George Washington Law Review*, 2013, n. 81, pp. 1574 e ss.

BANISAR D., DAVIES S., *Global trends in privacy protection: an international survey of privacy, data protection, and surveillance laws and development*, in *John Marshall Journal of Computer & Information Law*, vol. XVIII, 1999, n.1, pp. 44 e ss.

BARATTA T., *Le sopravvenienze e la clausola di rinegoziazione nei contratti di* outsourcing d*i sistema informatico tra buona fede e autonomia privata*, in P. PERLINGIERI (a cura di), *Rassegna di diritto civile*, vol. III, Napoli, Edizioni Scientifiche Italiane, 2018, pp. 800 e ss.

BARBIERATO D., *Dati personali e Internet*, Napoli, Edizioni Scientifiche Italiane, 2008, pp. 11 e ss.

BARBIERATO D., *Trattamento dei dati personali e "nuova" responsabilità civile,* in *Responsabilità Civile e Previdenza,* 2019, n. 6, pp. 2156 e ss.

BELLOMO G., *Contributo alla problematica della natura giuridica del "Data Protection Officer" (DPO*), marzo 2020*,* pp. 11 e ss., disponibile *online* su:

https://ricerca.unich.it/retrieve/e4233f17-76f2-2860-e053-6605fe0a460a/bellomo_scrittiCostanzo.pdf.

BELLUATI M., *Reti, spazi e culture. Verso nuovi orizzonti pubblici*, in F. CORBISIERO, E. RUSPINI (a cura di), *Sociologia del futuro. Studiare la società del ventunesimo secolo,* Padova, Cedam, 2016, pp.82 e ss.

BENATTI F., *Clausole di manleva*, in P. CENDON (a cura di), *Trattato di diritto civile*, Milano, Giuffrè, 2015, p. 291.

BERETTA M., RIZZA C., *Divieto di concentrazione e accordi di IT* outsourcing, in *Il Diritto Industriale*, 2004, n. 3, pp. 245 e ss.

BERLINGIERI M., *La responsabilità civile derivante dal trattamento dei dati personali:*
natura giuridica, conseguenze, oneri probatori, 2001, disponibile *online* su: https://www.privacy.it/archivio/berlingieri04.html.

BIANCA M., *Diritto Civile. L'obbligazione*, Milano, Giuffrè, 2019, pp. 709 e ss.

BIGNAMI F., *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*., vol. XLVIII, 2007, pp. 609 e ss.

BILOTTA F., *La responsabilità civile nel trattamento dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 456.

BISTOLFI C., BOLOGNINI L., PELINO E., *Il regolamento privacy europeo: commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, Giuffrè, 2016, pp. 125 e ss.

BLACK J., *Constitutionalising self-regulation*, in *The Modern Law Review*, vol. LIX, 1996, n. 1, pp. 24 e ss.

BOBAN M., *GDPR and Data Protection Impact Assessment (DPIA),* in M. MILKOVIC, K. HAMMES, O. BAKHTINA (a cura di), *Economic and Social Development (Book of Proceedings),* Varaždin, Varazdin Development and Entrepreneurship Agency, 2020, pp. 215 e ss.

BOTTA A. et al. alla "*International Conference on Future Internet of Things and Cloud Barcelona"* del 2014, dal titolo *"On the Integration of Cloud Computing and Internet of Things",* pp. 23 e ss., disponibile *online* su: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6984170.

BRADSHAW S., MILLARD C., WALDEN I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, in *International Journal of Law and Information Technology*, vol. IXX, 2011, n. 3, pp. 196 e ss.

BRAVO F., *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in N. Zorzi Galgano (a cura di), *Persone e Mercato dei Dati. Riflessioni sul GDPR*, Milano, Cedam, 2019, pp. 393 e ss.

BRAVO F., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di cassazione*, in *Contratto e Impresa*, 2023, n. 2, pp. 405 e ss.

BRODAHL L. et al., *EU Commission Publishes Template Data Processing Agreement*, giugno 2021, disponibile *online* su: https://www.wsgrdataadvisor.com/2021/06/eu-commission-publishes-template-data-processing-agreement.

BRUTTI N., *Le figure soggettive delineate dal GDPR: la novità del* Data Protection Officer, in E. TOSI (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali fra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, pp. 118 e ss.

BUKOVAC PUVAČA M., DEMARK A., *Pravo na zaštitu osobnih podataka kao temeljno pravo i odgovornost za štetu zbog njegove povrede*, in *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. XL, 2019, n. 1, pp. 287 e ss.

BURKERT H., *Privacy - Data Protection. A German/European Perspective*, in C. ENGEL, K.H. KELLER (a cura di), *Governance of Global Networks in the Light of Differing Local Values,* Baden Baden, Nomos Verlagsgesellschaft, 2000, pp. 43 e ss

BUSCA N., Cloud computing *e tutela della privacy nei rapporti commerciali B2B*, in *Studium Iuris*, 2020, n. 11, pp. 1327 e ss.

BUTTARELLI G., *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676*, Milano, Giuffrè, 1997, pp.71 e ss.

CAGGIANO I.A., *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio del diritto civile e commerciale*, 2018, n. 1, pp. 67 e ss.

CAGGIANO I.A., *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo e analisi comportamentale,* in *Annali-Università degli Studi Suor Orsola Benincasa,* vol. XI, 2021, n. 1, pp. 16 e ss.

CALZOLAIO S. et al., *La responsabilità e la sicurezza del trattamento*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/67,* Napoli, Editoriale scientifica, 2017, pp. 154 e ss.

CARDARELLI F., *La cooperazione fra le imprese nella gestione di risorse informatiche: aspetti giuridici del c.d.* <<outsourcing>>, in *Diritto dell'informazione e dell'informatica,* 1993, n.1, pp. 94 e ss.

CAREY P., *Data Protection: A Practical Guide to UK and EU Law*, Oxford, Oxford University Press, 2015, pp. 180 e ss.

CARLEO R., *Il principio di* accountability *nel GDPR: dalla regola alla auto-regolazione**, in CARLEO R., GAMBINO A.M., ORLANDI M. (diretto da), *Nuovo Diritto Civile*, 2021, n. 1, p. 373.

CASTRONOVO C., *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali*, in *Europa e diritto privato*, 1998, n. 3, p. 672.

CATERINA R., *Novità e continuità nel Regolamento generale sulla protezione dei dati*, in *Giurisprudenza Italiana*, 2019, n. 12, p. 2777.

CHEN J. et al., *Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption,* in *International Data Privacy Law,* vol. X, 2020, n. 4, pp. 281 e ss.

CHIAPPINI A., *Riflessioni sul contratto tra titolare e responsabile del trattamento*, in *Contratto e Impresa*, 2021, n. 1, pp. 317 e ss.

CICLOSI F., MASSACCI F., *The Data Protection Officer, a ubiquitous role nobody really knows*, in *IEEE Security and Privacy,* vol. XXI, 2022, n. 1, pp. 66 e ss.

ČIZMIĆ J., BOBAN M., *Učinak nove EU eredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj*, in *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, vol. XXXIX, 2018, n.1, pp. 382 e ss.

COCHRANE L., JASMONTAITE-ZANIEWICZ L., BARNARD-WILLS D., *Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises,* in *European Data Protection Law Review*, vol. VI, 2020, n. 3, pp. 353 e ss.

COLCELLI V., *Joint controller agreement under GDPR*, in *EU and Comparative Law Issues and Challenges Series*, 2019, n. 3, pp. 1038 e ss.

COLONNA V.*, Il sistema della responsabilità civile da trattamento dei dati personali*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali,* vol. II, Milano, Giuffrè, 2003, p. 10 e ss.

COMPORTI M., *Le presunzioni di responsabilità*, in *Rivista di Diritto Civile*, 2000, n. 5, pp. 660 e ss.

CORTESE B., *Commento all'art. 286 TCE,* in A. TIZZANO (a cura di), *Trattati dell'Unione e della Comunità Europea*, Milano, Giuffrè, 2004, pp. 1284 e ss.

CORTESE B., *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione Europea*, 2013, n. 2, p. 319.

D'ADDA A., *La solidarietà risarcitoria nel diritto privato europeo e l'art. 2055 c.c. italiano: riflessioni critiche*, in *Rivista di Diritto Civile*, 2016, n. 2, p. 303 e ss.

D'OTTAVIO A., *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, Giuffrè, 2019, pp. 172 e ss.

DE CONCEIÇÃO FREITAS M., MIRA DA SILVA M., *GDPR Compliance in SMEs: There is much to be done*, in *Journal of Information Systems Engineering & Management*, vol. III, 2018, n. 4, pp. 4 e ss.

DE RADA D., *La responsabilità civile per illecito trattamento dei dati ex art. 82 GDPR*, Santarcangelo di Romagna, Maggioli Editore, 2023, pp. 68 e ss.

DE STEFANI F., *Le regole della privacy. Guida pratica al nuovo GDPR*, Milano, Hoepli, 2018, pp. 19 e ss.

DE VITA A., *Il diritto all'autodeterminazione in ambito sanitario e il testamento biologico: verso nuove frontiere del diritto? Il diritto della sanità: problematiche attuali**, 2020, disponibile *online* su: https://www.giustizia-amministrativa.it/-/de-vita-il-diritto-all-autodeterminazione-in-ambito-sanitario-e-il-testamento-biologico-verso-nuove-frontiere-del-diritto-il-diritto-della-sanita-prob.

DEMETZOU K., *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, in E. KOSTA et al. (a cura di), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Berlino, Springer, 2019, pp. 137 e ss.

DI CIOMMO F., *Il danno non patrimoniale da trattamento dei dati personali*, in G. PONZANELLI (a cura di), *Il "nuovo" danno non patrimoniale*, Padova, Cedam, 2004, pp. 255 e ss.

DI CIOMMO F., *Vecchio e nuovo in materia di danno non patrimoniale da trattamento dei dati personali,* in *Danno e Responsabilità,* 2004, n. 10, pp. 817 e ss.

DI MAJO A., *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona,* cit., p. 238 ss.

DOTY N., MULLIGAN D. K., *Internet Multistakeholder Processes and Techno—Policy Standards. Initial Reflections on Privacy at the World Wide Web Consortium*, in *Journal on Telecommunications & High Technology Law*, 2013, n. 11, pp. 138 e ss.

DROBEK P., *The role of codes of conduct in the EU data protection framework*, in *GIS Odyssey Journal*, vol. II, 2022, n. 2, pp. 132 e ss.

DUCANGE L., *Patto di manleva e prescrizione del diritto del manlevato* Commento a Cass., 1° dicembre 2021, n. 37709 (ord.),* in *Pactum,* n. 3, 2022, pp. 383 e ss.

EDWARDS L. et al., *Data subjects as data controllers: a Fashion(able) concept?*, 2019, disponibile *online* su: https://discovery.ucl.ac.uk/id/eprint/10076025/1/EdwardsFinckVealeZingales.pdf

FACCIOLI E., CASSARO M., *Il "GDPR"e la normativa di armonizzazione nazionale alla luce dei principi:* accountability *e privacy* by design, in *Diritto industriale*, 2018, n. 6, pp. 563 e ss.

FARACE D., *Il titolare e il responsabile del trattamento*, in V. CUFFARO et al. (a cura di), *I dati personali nel diritto europeo*, Torino, Giappichelli, 2019, pp. 759 e ss.

FEDI A., *Diritto dell'impresa e protezione dei dati personali*, in *Società*, 2018, n. 10, pp. 1095 e ss.

FEKETE A., *What are privacy enhancing technologies? The 5 best PETs for the modern tech stack*, aprile 2022, disponibile *online* su: https://mostly.ai/blog/what-are-privacy-enhancing-technologies.

FERNANDEZ A., *EDPB Opinion 14/2019 on Standard Contractual Clauses for Processors under Article 28(8) GDPR*, in *European Data Protection Law Review,* n. 4, 2019, pp. 523 e ss.

FINOCCHIARO G., *Privacy e protezione dei dati personali. Disciplina e strumenti operativi,* Bologna, Zanichelli, 2012, p. 85.

FRANZONI M., *Responsabilità derivante da trattamento dei dati personali*, in G. FINOCCHIARO, F. DELFINI (a cura di), *Diritto dell'informatica,* Torino, UTET, 2014, p. 833.

GALIANO A. et al., *I dati non personali: la natura e il valore*, in *Rivista Italiana di Informatica e Diritto*, 2020, n. 1, pp. 61 e ss.

GAMBINO M., *Principio di responsabilità e tutela aquiliana dei dati personali*, in P. PERLINGIERI (diretto da), *Quaderni della Rassegna di diritto civile,* Napoli, Edizioni Scientifiche Italiane, 2018, pp. 135 e ss.

GARRI F., *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato,* in G. SANTANIELLO (a cura di), *La protezione dei dati personali*, Padova, Cedam, 2005, pp. 136 e ss.

GHAZIANI V. A., GHAZIANI M. A., GHAZIANI M. A., *Assessing Non-Material Damages Under the GDPR: A Review of The Recent Judicial Practice of Germany, UK, and the Netherlands*, in *Revista Jurídica Portucalense,* 2022, n. 32, pp. 280 e ss.

GIANNONE CODIGLIONE G., *Trattamenti multipli di dati personali e parcellizzazione degli obblighi di condotta*, in *Diritto dell'Informazione e dell'Informatica*, 2019, n. 6, pp. 1276 e ss.

GLEESON N., WALDEN I., "*It's a jungle out there"?: Cloud computing, standards and the law*", in *European Journal of Law and Technology,* vol. V, 2014, n. 2, pp. 21 e ss.

GLOBOCNIK J., *On Joint Controllership for Social Plugins and Other Third-Party Content– a Case Note on the CJEU Decision in Fashion ID*, in *International Review of Intellectual Property and Competition Law*, 2019, n. 50, pp. 1037 e ss.

GLON C., *Data Protection in the European Union: A Closer Look at the Current Patchwork of Data Protection Laws and the Proposed Reform That Could Replace Them All*, in *International Journal of Legal Information*, vol. XLII, 2014, n. 3, pp. 473 e ss.

GONZALEZ FUSTER G., GUTWIRTH S., *Opening up personal data protection: a conceptual controversy*, in *Computer Law & Security Review*, vol. XXIX, 2013, n. 5, pp. 531 e ss.

GORETTA R., *Risarcimento danni per violazione del GDPR, ecco chi paga e quanto***,** settembre 2019, disponibile *online* su: https://www.agendadigitale.eu/sicurezza/privacy/risarcimento-danni-per-violazione-del-gdpr-ecco-chi-paga-e-quanto/.

GRECO L., *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (diretto da), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, Zanichelli, 2017, pp. 278 e ss.

GRECO L., *L'organigramma privacy: I soggetti del trattamento*, in G. FINOCCHIARO (diretta da), *La protezione dei dati personali in Italia*. *Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, pp. 331 e ss.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP128), 22 novembre 2006, parr. 1 e 3.1, disponibile *online* su: https://ec.europa.eu/justice/article-29/en.pdf.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (WP 168), 1 dicembre 2009, par. 2.16, disponibile *online* su: https://ec.europa.eu/justice/article-29.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Parere 1/10 sui concetti di "responsabile del trattamento" e "incaricato del*

trattamento" (WP 169), 16 febbraio 2010, par. 3.1., lett. a, disponibile *online* su: https://www.privacy.it/archivio/grupripareri201001.html.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Parere 3/2010 sul principio di responsabilità* (WP 173), 13 luglio 2010, par. 2.21, disponibile *online* su: https://www.privacy.it/archivio/grupripareri201003.html#:~:text=Il%20Gruppo%20di%20lavoro%20art.%2029%20rileva%20che%20alcuni%20responsabili,difficile%20situazione%20economica%20dell'UE.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Parere 05/2012 sul* cloud computing *(WP 196*), 1 luglio 2012, par. 3.3.2, disponibile *online* su: https://www.privacy.it/archivio/grupripareri201205.html#:~:text=Nel%20suo%20parere%2C%20il%20Gruppo,cloud%20con%20clienti%20nel%20SEE.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (ART. 29), *Opinion 03/2013 on purpose limitation* (WP 203), 2 aprile 2013, par.2.1, disponibile *online* su: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE* (WP 217), 9 aprile 2014, parr. 1 e 2.4, disponibile *online* su: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti* (WP 223), 16 settembre 2014, p. 4, disponibile *online* su: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_it.pdf.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Guidelines on Data Protection Officers ('DPOs') (WP 243 rev.01),* 13 dicembre 2016, par. 12, disponibile *online* su: https://ec.europa.eu/newsroom/article29/items/612048.

GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI (Art. 29), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP 248 rev.01), 4 aprile 2017, par. 3, disponibile *online* su: https://ec.europa.eu/newsroom/article29/items/611236/en.

GUMZEJ N., *Selected aspects of proposed new EU general data protection legal framework and the Croatian perspective*, in *Juridical Tribune,* vol. III, 2013, n. 2, pp. 194 e ss.

GÜRSES S., TRONCOSO C., DIAZ C. alla "*Amsterdam Privacy Conference*" del 2015, dal titolo "*Engineering Privacy by Design Reloaded*", disponibile *online* su: http://carmelatroncoso.com/papers/Gurses-APC15.pdf.

HAQ S., BASHIR A., SHOLLA S., *Cloud of Things: Architecture, Research Challenges, Security Threats, Mechanisms and Open Challenges*, in *Jordanian Journal of Computers and Information Technology*, vol. VI, 2020, n. 4, pp. 420 e ss.

HARDING W. T., REED A. J., GRAY R. L., *Cookies and Web Bugs: What They Are and How They Work Together,* in R. HEROLD (a cura di), *The Privacy Papers*, Boca Raton, Auerbach Publications, 2001, pp. 351 e ss.

HÄRTING R.C., KAIM R., RUCH D., *Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design*, in *Agents and Multi-Agent Systems: Technologies and Applications, 14th KES International Conference*, Berlino, Springer, 2020, p. 295.

HOSSEIN MOTLAGH N. et al., *Internet of Things (IoT) and the Energy Sector*, in *Energies*, 2020, n. 13, pp. 494 e ss.

HU F., XIE D., SHEN S. alla "*IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*" del 2013, dal titolo "*On the Application of the Internet of Things in the Field of Medical and Health Care"*, pp. 2053 e ss, disponibile *online* su: https://www.computer.org/csdl/proceedings/greencom-ithingscpscom/2013/12OmNvk7JKB.

IMPERIALI R. E R., *Codice della Privacy*, Milano, Il Sole 24 Ore, 2004, pp. 196 e ss.

INCERTI A., *Il principio di limitazione della finalità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance, vol. I, Pisa, Pacini Giuridica, 2023, pp.203 e ss.

INFORMATION COMMISSIONER'S OFFICE, *Direct marketing detailed guidance*, 5 dicembre 2022, p. 10, disponibile *online* su: https://ico.org.uk/media/for-organisations/direct-marketing-guidance-and-resources/direct-marketing-guidance-1-0.pdf.

JAIN S., HALGAONKAR P. S., WADHAI V.M., *Review of RFID, NFC Technology and Its Applications,* in *International Journal of Engineering Research & Technology*, vol. III, 2014, n. 2.

JUSTY MIROBI G., AROCKIAM L. alla *"International Conference on Control, Instrumentation, Communication and Computational Technologies"* del 2015, dal titolo *"Service Level Agreement In Cloud Computing. An Overview"*, pp. 753 e ss., disponibile *online* su: https://ieeexplore.ieee.org/document/7475380.

KAMARA I., *Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation mandate*, in *European Journal of Law and Technology*, vol. VIII, 2017, n. 1, pp. 4 e ss.

KAMARINOU D., MILLARD C., TURTON F., *'Responsibilities of Controllers and Processors of Personal Data in Clouds',* in C. MILLARD (a cura di), *Cloud Computing Law,* Oxford, Oxford University Press, 2021, pp. 11 e ss.

KANDERP NARAYAN M. et al, *Survey on Internet of Things and its Application in Agriculture*, in *Journal of Physics: Conference Series 1714,* 2021, pp. 5 e ss.

KNETSCH J., *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, in *European Journal of Privacy Law & Technologies*, vol. XIII, 2022, n. 2, pp. 147 e ss.

KORFF D., *Report on the findings of the study*, in *EC Study on implementation of data protection directive*, n.3, 2002, pp.12 e ss.

KUAN HON W., *GDPR: Killing cloud quickly?,* marzo 2016, disponibile *online* su: https://iapp.org/news/a/gdpr-killing-cloud-quickly,

KUAN HON W., MILLARD C., WALDEN I., *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing*, in *International Data Privacy Law,* 2012, n. 1*,* pp. 14 e ss.

KUAN HON W., MILLARD C.,. SINGH J., *Twenty Legal Considerations for Clouds of Things,* in *Legal Studies Research Paper,* 2016, n. 216, pp. 9 e ss.

KÜCHLER H.F., *The Relations of Controllers, Processors and Sub-processors under the DPD and GDPR First Deliberations: Does the GDPR represent progress in the digital age?,* dicembre 2016, pp. 36 e ss., disponibile *online* su: https://www.duo.uio.no/bitstream/handle/10852/54570/ICTLTHESIS_8016.pdf.

KUNER C., *European Data Protection Law. Corporate Compliance and Regulation*, Oxford, Oxford University Press, 2007, pp. 46 e ss.

LEISER M.R., CUSTERS B.H.M, *THE Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680*, in *European Data Protection Law Review*, vol. V, 2019, n. 3, pp. 367 e ss.

LINDQVIST J., *New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?,* in *International Journal of Law and Information Technology*, 2018, n. 26, pp. 46 e ss.

LIPINSKI T. A., *Click Here to Cloud: End User Issues in Cloud Computing Terms of Service Agreements*, in *International Symposium on Information Management in a Changing World*, Berlino, Springer, 2013, pp. 92 e ss.

LOHSE E., *The Meaning of Harmonisation in the Context of European Union Law – a Process in Need of Definition*, in M. ANDENAS, C. ANDERSEN BAASCH (a cura di), *Theory and Practice of Harmonisation*, Cheltenham, Edward Elgar Publishing, 2012, p. 28.

LORÈ F.*, Il responsabile del trattamento. Privacy e "cura" dei dati in sanità*, in *Giornale Italiano di Nefrologia,* 2019, n. 2, pp. 5 e ss.

LOTTINI A., *Risarcimento del danno immateriale a seguito della violazione del regolamento (UE) 2016/679: la sentenza* Österreichische Post *determina un cambio di paradigma?,* in *Quaderni AISDUE*, 2023, n. 2, pp. 187 e ss.

LUCCHINI GUASTALLA E., *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori,* in *Contratto e Impresa*, 2018, n. 1, pp. 106 e ss.

LYNSKEY O., *Another Turn of the Screw? The 'Facebook Fanpages' judgment*, in *European Law Blog*, 2018, disponible *online* su: https://www.europeanlawblog.eu/pub/another-turn-of-the-screw-the-facebook-fanpages-judgment/release/1.

MADAKAM S., RAMASWAMY R., TRIPATH S., *Internet of Things (IoT): A Literature Review*, in *Journal of Computer and Communications*, 2015, n. 3, pp. 165 e ss.

MANGIAMELI S., relazione tenuta al IV Laboratorio Sublacense su "La comunità familiare e le scelte di fine vita" del 3-5 luglio 2009, dal titolo <<*Autodeterminazione: diritto di spessore costituzionale*>>, p. 1, disponibile *online* su: https://www.forumcostituzionale.it/wordpress/images/stories/pdf/documenti_forum/paper/0148_mangiameli.pdf,

MANTELERO A., *Processi di* outsourcing *informatico e* cloud computing*: la gestione dei dati personali ed aziendali*, in *Diritto dell'informazione e dell'informatica,* 2010, nn. 4-5, pp. 680 e ss.

MANTELERO A., *Il contratto per l'erogazione alle imprese di servizi di* cloud computing, in *Contratto e Impresa*, 2012, nn. 4-5, pp. 1216 e ss.

MANTELERO A., *Responsabilità aquiliana per uso della Rete e responsabilità del* provider*,* in F. DELFINI, G. FINOCCHIARO (a cura di), *Diritto dell'informatica,* Torino, UTET, 2014, pp. 823 e ss.

MANTELERO A., *Responsabilità e rischio nel Reg. UE 679/2016*, in *Le nuove leggi civili commentate*, 2017, n. 1, pp. 152 e ss.

MAROTTA A. et al., *Cyber - insurance survey*, in *Computer Science Review*, 2017, n. 24, pp. 35 e ss.

MASIERI C., *La tutela dei dati personali relativi alla salute: approccio europeo ed americano a confronto*, in R.E. CERCHIA (a cura di), *Percorsi di diritto comparato*, Milano, Milano University Press, 2021, pp. 199 e ss.

MASSIMINI M., *Il responsabile del trattamento*, febbraio 2006, pp. 2 e ss., disponibile *online* su: https://www.privacy.it/archivio/massimini01.html.

MELAND P. H. et al., *Facing Uncertainty in Cyber Insurance Policies,* in F. MARTINELLI, R. RIOS (a cura di), *Security and Trust Management,* Berlino, Springer, 2024.

MESSINA D., *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda* "Cambridge Analytica", in *federalismi.it,* 2018, n. 20, pp. 13 e ss.

MILLARD C. et al., *At this rate, everyone will be a [joint] controller of personal data*!, in *International Data Privacy Law*, vol. IX, 2019, n. 4, pp. 217 e ss.

MISCENIC E., HOFFMANN A.L., *The Role of Opening Clauses in Harmonization of EU Law: Example of the EU's General Data Protection Regulation (GDPR),* in *EU and Comparative Law Issues and Challenges series,* 2020, n. 4, pp. 52 e ss.

MLADINIĆ A., VUKIĆ Z., RONČEVIĆ A., *GDPR Compliance Challenges in Croatian Micro, Small and Medium Sized Enterprises*, in *Pravni vjesnik*, vol. XXXIX, 2023, nn. 3 - 4, pp. 68 e ss.

MORNET B., *L'indemnisation des Prejudices en cas de blessures ou de décès,* settembre 2021, disponibile *online* su: https://www.fac-droit.univ-smb.fr/wp-content/uploads/2022/10/Referentiel-dit-Mornet-septembre-2022.pdf.

MULLER M., *Die Öffnungsklauseln der Datenschutzgrundverordnung: Ein Beitrag zur Europäischen Handlungsformenlehre*, Münster, Wissenschaftliche Schriften der WWU, 2018, pp. 175 e ss.

MUSELLA A., *Il contratto di* outsourcing *del sistema informativo*, in *Diritto dell'informazione e dell'informatica,* 1998, n. 1, pp. 859 e ss.

MUSIO A., *Il principio di tolleranza nel diritto civile*, in *Contratto e Impresa*, 2017, n. 2, pp. 403 e ss.

MUSSAB A. et al., *A review of smart home applications based on Internet of Things*, in *Journal of Network and Computer Applications*, 2017, n. 97, pp. 48 e ss.

NADDEO F., *Il consenso al trattamento dei dati personali del minore*, in *Diritto dell'informazione e dell'informatica,* 2018, n. 1, pp. 27 e ss.

NAVONE G., *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Le Nuove Leggi Civili Commentate*, 2022, n. 1, p. 132 e ss.

NIST, *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, 2011, pp. 2 e ss., disponibile *online* su: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

NOTO LA DIEGA G., *Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom,* in *Journal of Law & Economic Regulation,* vol. IX, 2016, n. 1, pp. 79 e ss.

NOTO LA DIEGA G., WALDEN I., *Contracting for the 'Internet of Things': Looking into the Nest,* in *Queen Mary School of Law Legal Studies Research Paper,* 2016, n. 219.

O'BRIEN J., *GDPR series: Outsourcing contracts, all changed, changed utterly?,* in *Privacy e Data Protection,* vol. XVIII, 2018, n. 4, pp. 4 e ss.

O'DELL E., *Compensation for Breach of the General Data Protection Regulation*, in *Dublin University Law Journal (ns,)* vol. XL, 2017, n.1, pp. 21 e ss.

ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO, *Recommendation of the Council OECD Legal Instruments concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* OECD/LEGAL/0188, 23 settembre 1980, p. 8, disponibile *online* su: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf.

ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO, *The OECD Privacy Framework*, 2013, pp. 3 e ss., disponibile *online* su: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

PAGANO R., *Informatica e diritto*, Milano, Giuffrè, 1986, pp. 74 e ss.

PALMER V. V., *The Recovery of non- pecunary loss in European Contract Law,* in V.V. PALMER (a cura di), *The Common Core of European Private Law*, Cambridge, Cambridge University Press, vol. IV, 2015, pp. 4 e ss.

PANETTA R., *Gdpr, ecco chi sono (e cosa fanno) il* data controller *e il* data processor, marzo 2018, pp. 4 e ss., disponibile *online* su: https://www.corrierecomunicazioni.it/privacy/gdpr/gdpr-ecco-chi-sono-e-cosa-fanno-il-data-controller-e-il-data-processor/.

PITTALIS M., Outsourcing, in *Contratto e Impresa*, 2000, n. 2, pp. 1006 e ss.

PIZZETTI F., GRECO L., *Commento all'art. 26 Reg. 679/2016,* in R. D'ORAZIO et al. (a cura di), *Codice della Privacy e Data Protection,* Milano, Giuffrè, 2021, pp. 434 e ss.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, vol. I, Torino, Giappichelli, 2016, pp. 153 e ss.

POLETTI D., CAUSARANO M.C., *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI (a cura di), *Privacy Digitale,* Milano, Giuffrè, 2019, pp. 378 e ss.

POLETTI D., *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza Italiana*, 2019, n. 12, pp. 2787 e ss.

POLLICINO O., BASSINI M., *La Carta dei diritti fondamentali dell'Unione europea nel* reasoning *dei giudici di Lussemburgo*, in *Diritto dell'informazione e dell'informatica*, vol. XXXI, 2015, n. 4-5, pp. 77 e ss.

PRICE M., VERHULST S., *The Concept of Self-Regulation and the Internet*, in J. WALTERMANN, M. MACHILL (a cura di), *Protecting our children on the internet: Towards a new culture of responsibility*, Gütersloh, Bertelsmann Foundation Publishers, 2000, pp. 133 e ss.

QUELLEA C., *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk Based Approach*, in *European Journal of Risk Regulation*, vol. IX, 2018, n. 3, pp. 2 e ss.

RESTA G., SALERNO A., *La responsabilità civile per il trattamento dei dati personali*, in G. ALPA, G. CONTE (a cura di), *La responsabilità d'impresa*, Milano, Giuffrè, 2015, pp. 658 e ss.

RICCI A., *I diritti dell'interessato*, in G. FINOCCHIARO (diretta da), *La protezione dei dati personali in Italia*. *Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, pp. 394 e ss.

RICCI A., *L'*outsourcing *e* cloud computing, in F. DELFINI, G. FINOCCHIARO (a cura di), *Diritto dell'informatica*, Torino, UTET, 2014, pp. 672 e ss.

RICCIO G.M.*, Soggetti che effettuano il trattamento*, in S. SICA, P. STANZIONE (a cura di), *La nuova disciplina della privacy: commento al D.lgs. 30 giugno 2003, n. 196,* Zanichelli, Bologna, 2004, pp. 123 e ss.

RICCIO G. M., *Titolarità e contitolarità dei dati personali alla luce della decisione della Corte di giustizia sulle* fanpage *di Facebook*, in *MediaLaws*, 2018, n. 3, pp. 352 e ss.

RICCIO G.M., *Titolarità e contitolarità nel trattamento dei dati personali tra Corte di Giustizia e Regolamento privacy,* in *Nuova Giurisprudenza Civile Commentata*, 2018, n. 12, pp. 1805 e ss.

RICCOBENE A., *Il danno cagionato per effetto del trattamento e i diversi modelli risarcitori*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali,* vol. II, Milano, Giuffrè, 2006, pp. 2021 e ss.

RICKNÄS M., *Google Apps deal disallowed by Swedish data regulator*, 10 giugno 2013, disponibile *online* su: https://www.pcworld.com/article/452338/google-apps-deal-disallowed-by-swedish-data-regulator.html.

RIPLEY C., *The importance of appropriate liability caps,* maggio 2024, disponibile *online* su: https://www.fsp-law.com/the-importance-of-appropriate-liability-caps/.

ROHRMANN C. A., FALCI SOUSA ROCHA CUNHA J., *Some Legal Aspects of Cloud Computing Contracts*, in *Journal of International Commercial Law and Technology*, vol. X, 2015, n. 1, p. 40.

RUBINO D., IUDICA G., *Appalto*, in F. GALGANO (a cura di), *Commentario al codice civile Scialoja – Branca*, Bologna, Zanichelli, pp. 26 e ss.

RUFFOLO U., *Dati personali: trattamento e responsabilità*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffrè, 1998, p. 284 e ss.

SAJFERT J., *Croatia: Minimum Service for the Implementation, Big Service to the Public Sector*, in *European Data Protection Law Review*, vol. VI, 2020, n. 2, pp. 281 e ss.

SALAMI E., *Examining the legality of limitation of liability clauses under the GDPR*, in *Computer and Telecommunications Law Review*, vol. XXIV, 2018, n. 8, pp. 175 e ss.

SALVI C., *Responsabilità extracontrattuale (dir. vig.),* in *Enciclopedia del diritto*, vol. XXXIX, Milano, Giuffrè, 1988, pp. 1234 e ss.

SAMMARCO P., *I nuovi contratti dell'informatica. Sistema e prassi*, in F. GALGANO (a cura di), *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, Cedam, 2006, pp. 403 e ss.

SAVONARDO L., *Pop music, media e culture giovanili: dalla* Beat Revolution *alla* Bit Generation, in *Convergenze culturali*, Milano, EGEA, 2017, p.110.

SCHINELLI A., *Profili critici del trasferimento di dati personali UE-USA tra conflitti regolatori e reazioni politiche*, in S. BONAVITA (a cura di), *Società delle tecnologie esponenziali e* General Data Protection Regulation*: la circolazione internazionale dei dati personali*, Milano, Ledizioni, 2018, pp. 2 e ss.

SCHMIDT A., VAN LEARHOVEN K., *How to Build Smart Appliances*?, in *IEEE Personal Communications*, vol. VIII, 2021, n. 4, pp. 66 e ss.

SCHONHOFEN S., WILDE-DETMERING F., HARDINGHAUS A., *German court ruling: no claims for damages under Article 82 GDPR for minor GDPR violations*, 21 agosto 2019, disponibile *online* su: https://www.technologylawdispatch.com/2019/08/in-the-courts/german-court-ruling-no-claims-for-damages-under-article-82-gdpr-for-minor-gdpr-violations/.

SCHWEIGER T., *Die Post bringt allen was .... oder: „es stört mich, dass meine Daten verarbeitet werden."*,11 ottobre 2019, disponibile *online* su: https://www.dataprotect.at/parteienaffinit%C3%A4t-und-schadenersatz/.

SICA S., D'ANTONIO V., *I Safe Harbor Privacy Principles: genesi, contenuti, criticità,* in *Diritto dell'informazione e dell'informatica,* vol. XXXI, 2015, n. 4-5, pp. 80 e ss.

SICA S., GIANNONE CODIGLIONE G.*, La libertà fragile. Pubblico e privato al tempo della rete*, Napoli, Edizioni Scientifiche Italiane, 2014, pp. 25 e ss.

SICA S., STANZIONE P. (a cura di), *La nuova disciplina della privacy - d.lgs. 20 giugno 2003, n. 196,* Bologna, Zanichelli, 2004, pp. 123 e ss.

SOFFIENTINI M., *Privacy. Protezione e trattamento dei dati*, Assago, IPSOA, 2018, pp. 4 e ss.

SPINA A., *Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al Regolamento (UE) 2016/67,* in *Rivista della Regolazione dei mercati*, 2016, n. 1, p. 148.

STABILE S., *Le nuove frontiere della pubblicità e del* marketing *su internet*, in *Diritto Industriale*, 2009, n. 5, pp. 482 e ss.

STANZIONE M.G., *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Diritto privato*, 2016, n. 4, pp. 1249 e ss.

STYLIANOU K., VENTURINI J., ZINGALES N., *Protecting user privacy in the Cloud: an analysis of terms of service*, in *European Journal of Law and Technology*, vol. VI, 2015, n. 3.

SZALOWSKI R.*, Data Protection Officer in the light of the provisions of the General Data Protection Regulation (GDPR*), in *Ius Novum*, 2018, n.4, pp. 120 e ss.

TAMBOU O., *Opening Remarks*, in K. MC CULLAGH et al. (a cura di), *National Adaptations of the GDPR,* Lussemburgo*,,* Collection Open Access Book, 2019, pp. 24 e ss.

TENE O., *Privacy: The new generations*, in *International Data Privacy Law*, vol. I, 2011, n.1, pp. 15 e ss.

TESAURO G., *Diritto Comunitario*, Cedam, Padova, 2001, p. 118.

TOMMASEO F.*, Rappresentanza e difesa del minore nel processo civile*, in *Famiglia e Diritto,* 2007, n. 4 p. 411 e ss.

TORASSA COLOMBERO V., ROATTA S., LOPEZ P., *Botnets: Estado del arte y taxonomía de una amenaza sigilosa*, in *SACS - Simposio Argentino de Ciberseguridad y Ciberdefensa,* vol. X, 2024, n. 7, pp. 62 e ss.

TORINO R., *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679,* in *La cittadinanza europea,* 2018, n. 2, pp. 50 e ss.

TOSI F., *Il contratto di* outsourcing *di sistema informatico*, Milano, Giuffrè, 2001, pp. 5 e ss.

TOSI E., *Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: Funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo,* in *Contratto e Impresa*, 2020, n. 3, pp. 1134 e ss.

TOSI E., *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale,* Milano, Giuffrè, 2020, pp. 253 e ss.

TOSI E., *Diritto privato delle nuove tecnologie digitali. Riservatezza, contratti, responsabilità fra persona e mercato,* in V. FRANCESCHELLI, E. TOSI (diretto da), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2021, pp. 568 e ss.

TRONCOSO REIGADA A., *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Cívitas, 2010.

TUNG L., *Sweden tells council to stop using* Google Apps, 14 giugno 2013, disponibile *online* su: https://www.zdnet.com/article/sweden-tells-council-to-stop-using-google-apps/.

UNCITRAL*, Notes on the Main Issues of Cloud Computing Contracts*, 2019, pp. 30 e ss., disponibile *online* su: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09103_eng.pdf.

VALLE L. et al., *Struttura dei contratti e trattamento dei dati personali nei servizi di* cloud computing *alla luce del nuovo Reg. 2016/679 UE*, in *Contratto e Impresa – Europa*, 2018, n. 1, pp. 347 e ss.

VAN ALSENOY B., *Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation*, in *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. VII, 2016, n. 3, pp. 273 e ss.

VISINTINI G., *Inadempimento e mora del debitore. Artt. 1218 -1222*, in *Commentario Schlesinger,* Milano, Giuffrè, 2006, pp. 94 e ss.

VIZZONI L.*, Domotica e diritto. La* Smart Home *tra regole e responsabilità*, in V. FRANCESCHELLI, E. TOSI (diretto da), *Diritto delle nuove tecnologie*, Milano, Giuffrè, 2021, pp. 81 e ss.

WEBER R.H, WEBER R., *Internet of Things. Legal Perspectives*, Berlino, Springer, 2010, pp. 17 e ss.

WESTIN A.F., *Privacy and Freedom,* New York, Atheneum, 1967, pp. 7 e ss.

ZELL A. M., *Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field German Law*, in *German Law Journal*, vol. XV, 2014, n. 3, pp. 461 e ss.

ZENCOVICH Z., ZOPPINI A., *La disciplina dei servizi telematici nel quadro delle proposte comunitarie di tutela dei dati personali*, in *Diritto dell'informazione e dell'informatica*, 1992, n. 3, p.773.

ZIEGENHORN G., FOKKEN M., *CGUE: ambito di responsabilità per la protezione dei dati dei gestori di siti web,* 2019, disponibile *online* su: https://www.redeker.de/de/newsletter/gewerblicher-rechtsschutz-medienrecht-und-datenschutz-2-2019.

ZIVIZ P., *Trattamento dei dati personali e responsabilità civile: il regime previsto dalla Legge 675/1996*, in *Responsabilità civile e previdenza*, 1997, pp. 1307 e ss.

Giurisprudenza citata

Sentenze della Corte di Giustizia

Corte giust. UE 14 maggio 1998, C-259/96, *Council of the European Union v. Lieva de Nil and Christiane Impens*, disponibile *online* su: www.curia.europa.it.

Corte giust. UE 11 dicembre 2014, C-212/13, *František Ryneš contro Úřad pro ochranu osobních údajů,* in *Diritto, Mercato, Tecnologia*, 2015, n. 3, con nota di D. B. Casiere, *La videosorveglianza ad uso domestico: ambito di applicazione della direttiva europea in materia di protezione dei dati personali.*

Corte giust. UE 6 ottobre 2015, C-362/14, *Maximilian Schrems v. Data Protection Commissioner*, disponibile *online* su: www.curia.europa.it.

Corte giust. UE 4 aprile 2017, C-337/15 P, *European Ombudsman v. Claire Staelen*, disponibile *online* su: www.curia.europa.it.

Corte giust. UE 5 giugno 2018, C-210/16*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, disponibile *online* su: https://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=IT.

Corte giust. UE 29 luglio 2019, C-40/17*, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW e V,* disponibile *online* su: https://curia.europa.eu/juris/document/document.jsf;jsessionid=CE0C6EA78A43FA822FDAB77E760ED473?text=&docid=216555&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=10620378.

Corte giust. UE 4 maggio 2023, C-300/21, *UI v.* Österreichische Post AG, in *Foro it.*, 2023, IV, 268 ss., con nota di A. PALMIERI, R.

PARDOLESI, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, c. 278 e ss.

Corte giust. UE 25 gennaio 2024, C-687/21*, BL contro* MediaMarktSaturn Hagen-Iserlohn GmbH, disponibile *online* su: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62021CJ0687

Sentenze della Corte di Cassazione

Cass. 23 febbraio 1983, n. 1394, in *Mass. Giur. it.*, 1983.

Cass. 11 novembre 2008, n. 26972, in *Rep. Foro It*., 2008, voce *Danni in materia civile*, n. 309.

Cass. sez. un. 11 novembre 2008, nn. 26972, 26973, 26975, in *Dir. fam. pers*., 2009, I, 73 con nota di F. GAZZONI, *Il danno esistenziale, cacciato, come meritava, dalla porta, rientrerà dalla finestra*.

Cass. 17 aprile 2012, n. 5997, in *Argomenti di Diritto del Lavoro*, 2012, 4, 974, con nota di A. RICCOBONO, *Verso una tipizzazione del "contratto di esternalizzazione"*?,

Cass. 8 aprile 2014, n. 8184, in *Rep. Foro It.,* 2014, voce *Persona fisica e diritti della personalità*, n.124.

Cass. 11 giugno 2014, n. 13219, in *Responsabilità Civile e Previdenza,* 2014, n. 4, 1357.

Cass. 15 luglio 2014, n. 16133, in *Danno e resp.,* 2015, 339*,* con note di V. CECCARELLI, *La soglia di risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*; M. NITTI, *La valutazione della "gravita` della lesione" e della "serieta` del danno" nel risarcimento del danno non patrimoniale da violazione della privacy.*

Cass. 5 settembre 2014, n. 18812, *in Foro it.*, 2015, I, 119.

Cass. 19 settembre 2014, n. 19834, *in Rep. Foro it.,* 2014*,* voce *Locazione,* n. 75.

Cass. 5 marzo 2015, n. 4443, in *Rep. Foro it*., 2015, voce *Spese giudiziali in materia civile,* n. 78.

Cass. 11 gennaio 2016, n. 222, in *Dir. e giust.,* 2016, 12, con nota di M. ALOVISIO, *Risarcimento del danno per diffusione indebita di dati sanitari.*

Cass. 8 gennaio 2019, n. 207, in *Massimario.it*, 2019, VI, con nota di M. E. BAGNATO, *Illecita segnalazione alla Crif? Il danno deve essere provato dall'interessato.*

Cass. 20 agosto 2020, n. 17383, in *Dir. Internet*, 2020, 619, con nota di A. AVITABILE*, Il risarcimento del danno a seguito dell'illecito trattamento di dati personali: un nuovo impulso dal reg. UE 27 aprile 2016 n. 679.*

Cass. 12 maggio 2023, n. 13073, in *Nuova giur. civ. comm.,* 2023, V, p. 1125, con nota di G.M. RICCIO, *Dati personali e rimedi: diritti degli interessati e profili risarcitori.*

Sentenze delle Corti di merito

Tribunale di Reggio Calabria, 25 febbraio 2020, con commento di A. SOUIHEL, V. ZANNI, *Risarcimento danni privacy: l'Ue allarga le maglie, l'Italia resta cauta*, settembre 2024, disponibile *online* su: https://www.agendadigitale.eu/sicurezza/privacy/risarcimento-danni-privacy-lue-allarga-le-maglie-litalia-resta-cauta/.

Sentenze di Corti straniere

Court of Appeal of London, 27 marzo 2015, n. A2/2014/0403, disponibile *online* su: https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf.

Supreme Court of the Netherlands, 9 maggio 2003, n. C01/246HR, disponibile *online* su: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2003:AF4606.

Supreme Court of the Netherlands, 15 marzo 2019, n. 17/04668, disponibile *online* su: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2019:376.

Tribunale distrettuale di Amsterdam, 2 settembre 2019, n. 7560515 CV ESPL 19-4611, disponibile *online* su: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2019:6490.

Tribunale distrettuale di Noord-Nederland, 15 gennaio 2020, n. C/18/189406/HA SAB 19-6, disponibile *online:* su https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNNE:2020:24.

Tribunale locale di Diez, 7 novembre 2018, n. 8 C 130/18, disponibile *online* su: https://openjur.de/u/2116788.html.

Tribunale regionale superiore di Dresda, 11 giugno 2019, n. 4 U 760/19, disponibile *online* su: https://openjur.de/u/2316062.html.

Tribunale regionale di Karlsruhe, 2 agosto 2019, n. 8 O 26/19. In merito, v. *LG Karlsruhe: Kein Schadensersatz-Anspruch nach der DSGVO aus generalpräventiven Gründen*, 5 novembre 2019, disponibile *online* su:

https://www.dr-bahr.com/news/kein-schadensersatz-anspruch-nach-der-dsgvo-aus-generalpraeventiven-gruenden.html.

Tribunale regionale di Monaco I, 7 novembre 2019, n. 34 O 13123/19, disponibile *online* su: https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2019-N%2028276?hl=true&fontsize=small.

Tribunale regionale superiore di Innsbruck, 13 febbraio 2020, n. 1 R 182/19b, disponibile *online* su: https://www.dataprotect.at/2020/03/06/post-schadenersatz/.

Tribunale regionale di Feldkirch, 14 agosto 2019, n. 57 Cg 30/19b, disponibile *online* su: file:///C:/Users//Downloads/Urteil-LG-Feldkirch-O%CC%88sterreichische-Post-AG-anonymisiert-online%20(4).pdf.

Tribunale distrettuale di Overijssel, 28 maggio 2019, n. AK_18_2047, disponibile *online* su: https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBOVE:2019:1827.

Županijski sud u Zagrebu, 28 marzo 2017, Gžn -748/13-7, disponibile *online* su: https://www.iusinfo.hr/sudska-praksa/ZSRH201374B8A7.

Decisioni citate di autorità amministrative indipendenti

Decisioni del Garante europeo per la protezione dei dati

Garante europeo per la protezione dei dati, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union"*, 14 gennaio 2011, par. 5.5, disponibile *online* su: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/comprehensive-approach-personal-data-protection_en

Garante europeo per la protezione dei dati, *Relazione Annuale 2015 - Sintesi*, pp. 4 e ss., disponibile *online* su: https://www.edps.europa.eu/sites/default/files/publication/ar2015_summary_it.pdf

Garante europeo per la protezione dei dati, *Opinion on coherent enforcement of fundamental rights in the age of big data*, 23 settembre 2016, par. 2.1., disponibile *online* su: https://www.edps.europa.eu/sites/default/files/publication/16-09-23_bigdata_opinion_en.pdf.

Decisioni del Garante della protezione dei dati delle istituzioni dell'Unione Europea

Garante della protezione dei dati delle istituzioni dell'Unione Europea (EDPS), *EDPS Guidelines on the concepts of controller, processor and joint controllership*

under Regulation (EU) 2018/1725, 7 novembre 2019, pp. 27 e ss., disponibile *online* su: https://www.edps.europa.eu/sites/default/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf.

Decisioni del Garante per la protezione dei dati personali

Garante per la protezione dei dati personali, *Chiarimenti sulla Circolare n. 291/S del 13 novembre 1997 recante direttive in materia di protezione dei dati personali*, 9 dicembre 1997, pp.1 e 2, disponibile *online* su: https://www.privacy.it/archivio/garanterisp199712092.html.

Garante per la protezione dei dati personali, *Stato di attuazione del Codice in materia di protezione dei dati personali - Relazione 2004 - 9 febbraio 2005*, par. 1.1., disponibile *online* su: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1093797.

Garante per la protezione dei dati personali, *Trattamento dei dati personali attraverso un sistema "Rfid" di monitoraggio a distanza di pazienti portatori di defibrillatori cardiaci impiantabili attivi. Verifica preliminare richiesta da Azienda Ospedaliera e Sas - 29 novembre 2012 [2276103]*, disponibile *online* su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2276103.

Garante per la protezione dei dati personali, *Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali*, febbraio 2018, pp. 23 e ss., disponibile *online* su: https://www.unich.it/sites/default/files/guida_all_applicazione_del_regolamento_ue_2016_679.pdf.

Garante per la protezione dei dati personali, Accountability *(responsabilizzazione). Approccio basato sul rischio e misure di* accountability*(responsabilizzazione) di titolari e responsabili*, disponibile *online* su: https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di%20accountability-responsabilizzazione-di-titolari-e-responsabili.

Garante per la protezione dei dati personali, *Cosa intendiamo per dati personali? *,* disponibile *online* su: https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali.

Decisioni delle Autorità nazionali per la protezione dei dati

Agencija za zastitu osobnih podataka (AZOP), *Report on activities for 2012 - Izvjesce o radu za 2012. godinu*, giugno 2012, pp. 24 e ss., disponibile *online* su: https://azop.hr/wp-content/uploads/2020/12/Izvjesce_o_radu_AZOP_za_2012.pdf.

Agencija za zastitu osobnih podataka (AZOP), *Ugovor o obradi podataka između voditelja obrade i izvršitelja obrade prema članku 28. st. 3.Opće uredbe o zaštiti podataka sklapa se između,* 9 dicembre 2022, disponibile *online* su: https://azop.hr/wp-content/uploads/2023/03/Ugovor-o-obradi-podataka-izmedu-voditelja-obrade-i-izvrsitelja-obrade-prema-clanku-28-OUZP-template.docx

Agencija za zastitu osobnih podataka (AZOP), *Uloga voditelja i izvršitelja obrade (zaposlenici voditelja obrade nisu izvršitelji obrade)*, 20 marzo 2023, disponibile *online* su: https://aop.hr/uloga-voditelja-i-izvrsitelja-obrade-zaposlenici-voditelja-obrade-nisu-izvrsitelji-obrade/.

Agencija za zastitu osobnih podataka (AZOP), *Razgraničenje uloge voditelja obrade i izvršitelja obrade*, disponibile *online* su: https://azop.hr/voditelj-i-izvrsitelj-obrade/.

Datatilsynet, *Standardkontraktsbestemmelser vedtaget af Datatilsynet*, dicembre 2019, disponibile *online* su: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/dec/standardkontraktsbestemmelser-vedtaget-af-datatilsynet/.

Integritetsskyddsmyndigheten (IMY), *Tillsyn enligt personuppgiftslagen (1998:204) – Uppföljning av beslut i ärende 263-2011,* 31 maggio 2013, par. 1.2, disponibile *online* su: https://www.imy.se/globalassets/dokument/beslut/2013-/2013-05-31-salems-kommun.pdf.