COLLANA L'UNITÀ DEL DIRITTO 54

IL VALORE DEL DISSENSO

Riflessioni con Vincenzo Zeno-Zencovich

VOLUME II

a cura di FRANCESCO CARDARELLI, TOMMASO EDOARDO FROSINI, ELISE POILLOT, GIORGIO RESTA, SALVATORE SICA, ANDREA ZOPPINI

RomaTrE-Press
2025

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

COLLANA L'UNITÀ DEL DIRITTO 54

IL VALORE DEL DISSENSO

Riflessioni con Vincenzo Zeno-Zencovich

VOLUME II

a cura di
FRANCESCO CARDARELLI, TOMMASO EDOARDO FROSINI, ELISE POILLOT,
GIORGIO RESTA, SALVATORE SICA, ANDREA ZOPPINI

Roma TrE-Press
2025

La Collana *L'unità del diritto* è stata varata su iniziativa dei docenti del Dipartimento di Giurisprudenza. Con questa Collana si intende condividere e sostenere scientificamente il progetto editoriale di Roma Tr*E-Press*, che si propone di promuovere la cultura giuridica incentivando la ricerca e diffondendo la conoscenza mediante l'uso del formato digitale ad accesso aperto.

Collana pubblicata nel rispetto del Codice etico adottato dal Dipartimento di Giurisprudenza dell'Università degli Studi Roma Tre, in data 22 aprile 2020.

Il volume pubblicato è stato sottoposto a previa e positiva valutazione nella modalità di referaggio *double-blind peer review.*

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: MOSQUITO. mosquitoroma.it

Caratteri tipografici utilizzati:
Day Roman, Iowan Old Style (copertina e frontespizio)
Adobe Garamond Pro (testo)

Impaginazione e cura editoriale: Colitti-Roma colitti.it

Edizioni: Roma TrE-Press
Roma, dicembre 2025
ISBN: 979-12-5977-544-3
http://romatrepress.uniroma3.it

L'attività della *Roma TrE-Press* è svolta nell'ambito della
Fondazione Roma Tre-Education, piazza della Repubblica 10, 00185 Roma

Sezione IV
Responsabilità civile

Mario Renna

Violazione dei dati personali, principio di sicurezza e responsabilità

Sommario: 1. *Data loss* e violazione dei dati personali – 2. Sicurezza dei dati personali: evoluzioni disciplinari – 3. Spunti a partire dal caso VB c. Natsionalna agentsia za prihodite – 4. *Data breach*: trasparenza e reazione – 5. Le *Guidelines 9/2022 on personal data breach notification under GDPR* – 6. Considerazioni conclusive.

1. Data loss *e violazione dei dati personali*

In uno scritto del 2024, il Professore Vincenzo Zeno-Zencovich si è soffermato sul significato, nonché sulla rilevanza giuridica, del fenomeno traducibile mediante la locuzione «data loss»[1]; nell'ambito dei rapporti tra utenti e *service providers*, ha osservato, si è soliti riscontrare «a flourish of clauses which exclude any sort of liability»[2]. Al di là dei rapporti contrattuali - e delle relative clausole concernenti la perdita dei dati - intercorrenti tra utenti, nelle vesti di consumatori ovvero di non consumatori, e *service providers*, l'A. ha registrato come, a livello di responsabilità extracontrattuale, «it is still unclear what the arguments for and the consequences of civil liability for the loss of data (or for the loss of access to data) will be»[3].

Il fenomeno della perdita di dati interessa soprattutto i dati personali e il Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, sin d'ora GDPR, offre una precisa definizione della violazione dei dati personali, fattispecie che ingloba anche la perdita dei dati, delimita le responsabilità di titolare e responsabile del trattamento e si accredita quale sistema normativo di riferimento: come ha notato l'A., «from a practical point one can easily imagine that natural persons will prefer to bring their claim on the basis

[1] V. Zeno-Zencovich, *Liability for data breaches and losses*, in V. Mak, E. Tjong Tjin Tai, A. Berlee (eds.), *Research Handbook in Data Science and Law*, Edward Elgar, Cheltenham-Northampton 2024, pp. 77-79.
[2] *Ivi*, pp. 82-83.
[3] *Ivi*, p. 86.

of such explicit norms, rather than engaging in academic qualifications on the notion of data and of their legal relevance. This approach is prompted by a "catch-all" approach by DPAs which, when sanctioning controllers for not having introduced adequate security measures against data breaches, do not make much difference on the type of data that have been destroyed or misappropriated».[4].

Il GDPR posiziona la sicurezza tra i principi applicabili al trattamento dei dati personali, quindi al vertice della regolamentazione giuridica[5]: i dati personali necessitano di essere trattati in maniera tale da assicurare una adeguata sicurezza e una costante integrità e riservatezza [art. 5, par. 1, lett. *f*)]. Il principio di sicurezza si atteggia a dispositivo giuridico che necessita di una concretizzazione puntuale e, al contempo, favorisce l'emergere di una serie di responsabilità gravanti sul titolare e sul responsabile del trattamento[6]. Per costoro si impone una valutazione costante e prudente dei rischi[7]: con riferimento ad ogni fase dell'attività del trattamento dei dati, si configura un dovere di mantenimento di un livello di sicurezza adeguato ai rischi, articolato in obblighi di prevenzione e reazione. Un primo e sommario esame del GDPR, oltre a censire l'incrementato impatto della *liability rule* e l'affermarsi di un processo di *accountability* - basti

[4] *Ivi*, p. 87.

[5] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[6] Per una utile sintesi e un aggiornato compendio delle decisioni più significative assunte dalle Autorità domestiche competenti, v. E. Kosta, *Security of Processing and Data Breach Notification*, 18 gennaio 2024, in *edpb.europa.eu/our-work-tools/our-documents/support-pool-expert-projects/one-stop-shop-case-digest-security_en.*

[7] Sulla risarcibilità dei danni da violazione del GDPR, v. Corte giust., 4 maggio 2023, C-300/21, *UI c. Österreichische Post AG*, con commenti di C. Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, di S. Patti, *Il risarcimento del danno immateriale secondo la Corte di giustizia* e di C. Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, tutti in *Nuova giur. civ. comm.*, fasc. 2, 2023, rispettivamente a p. 1136 ss., p. 1146 ss., p. 1150 ss.; nonché di A. Palmieri, R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della* privacy *(purché lo si provi!)*, di S. Pagliantini, *Un altro palcoscenico della «guerra» tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr* e di 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*, tutti in *Foro it.*, fasc. 4, 2023, rispettivamente a p. 278 ss., p. 285 ss., p. 293 ss. Per maggiori riferimenti, cfr. U. Salanitro, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.*, fasc. 3, 2023, p. 426 ss.; S. Thobani, R. Caterina, *Il diritto al risarcimento dei danni*, in *Giur. it.*, fasc. 12, 2019, p. 2805 ss.; F. Mezzanotte, *Risk Allocation and Liability Regimes in the IoT*, in A. De Franceschi, R. Schulze (eds.), *Digital Revolution – New Challenges for Law Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, BECK-Nomos, München 2019, p. 182 ss.

pensare alla protezione dei dati *by design* e *by default*, *ex* art. 25 GDPR -, consente di cogliere una sostenuta elevazione del livello di protezione dei diritti e delle libertà delle persone fisiche[8].

2. *Sicurezza dei dati personali: evoluzioni disciplinari*

La sicurezza, come può ricavarsi dalla lettura della Convenzione di Strasburgo n. 108/81, «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», non ha costituito, solamente, un canone operativo dell'attività del trattamento dei dati[9], assurgendo, invero, a principio fondamentale[10]. Ai sensi del testo originario dell'art. 7, «adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate». Anche successivamente alle modifiche apportate alla Convenzione attraverso il Protocollo del Consiglio d'Europa del 17 e 18 maggio 2018, la sicurezza non ha smarrito la sua qualificazione di principio ordinatore[11].

[8] Cfr. A. Mantelero, G. Vaciago, *Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector*, in R. Senigaglia, C. Irti, A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Springer, Singapore 2022, p. 97 ss.; T. Sica, *Cybersecurity and risk management*, in *Corporate governance*, 2022, p. 581 ss.; P. Laghi, *Struttura della rete e responsabilità: cybersecurity*, in *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Edizioni Scientifiche Italiane, Napoli 2020, p. 255 ss.; E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Giuffrè, Milano 2019, spec. p. 73 ss.

[9] S. Rodotà, *Elaboratori elettronici e controllo sociale*, il Mulino, Bologna 1973, p. 81 ss.; Id., *Protezione dei dati e circolazione delle informazioni*, in Id. (a cura di), *Tecnologie e diritti*, il Mulino, Bologna 1995, p. 41 ss.; V. Frosini, *Diritto alla riservatezza e calcolatori elettronici*, in G. Alpa, M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Cedam, Padova 1984, p. 29 ss.; G. Corasaniti, *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano 2003.

[10] S. Rodotà, *Tecnologie dell'informazione e frontiere del sistema socio-politico*, in G. Alpa, M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, cit., p. 89 ss.

[11] Con riguardo alla sicurezza nel trattamento nell'ambito dei sistemi di National Digital Identity, intesi alla stregua di «a combination of policy, law, and technology by which a person's personal data are captured to establish and digitally represent, verify and manage a person's legal identity across public (and private) services identified in national policy and

Tuttavia, la Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[12], risultò disallineata rispetto alla Convenzione di Strasburgo, in quanto la sicurezza venne degradata a mera regola di condotta, il cui rispetto doveva essere esclusivamente assicurato dal responsabile del trattamento (art. 17)[13]. Veniva prescritta l'adozione di misure tecniche e organizzative appropriate e capaci di assicurare la protezione dei dati personali rispetto a ipotesi di distruzione accidentale o illecita, di perdita accidentale o alterazione, diffusione o accesso non autorizzati, nonché dinanzi al rischio di qualsivoglia forma illecita di trattamento dei dati, con particolare riguardo al trattamento concernente trasmissioni di dati in rete.

Nel testo della l. n. 675/1996, dedicata alla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, la sicurezza non comparve tra le finalità della normativa e, al contempo, non rappresentò un principio per il trattamento dei dati. Tale scelta ebbe delle ricadute in termini di tutela delle posizioni giuridiche soggettive incise dal trattamento dei dati: non fu conferito all'interessato un diritto ad ottenere una tutela anticipatoria, venendo individuato nel solo rimedio risarcitorio lo strumento atto a ricomporre le perdite patite per via della violazione della disciplina della sicurezza[14]. L'adozione di misure di sicurezza era correlata allo stato di conoscenze acquisite in base al progresso tecnico[15]: la custodia e il controllo dei dati, in ragione di ciò, dovevano essere calibrati rispetto alla natura dei dati medesimi e alle specifiche caratteristiche del trattamento.

law», v. le *Guidelines on National Digital Identity*, The Council of Europe, 18 novembre 2022, par. 3.6.

[12] V. Zeno-Zencovich, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*", in V. Cuffaro, V. Ricciuto, Id. (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, Milano 1998, p. 159 ss.

[13] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino 2019, p. 809.

[14] Secondo S. Rodotà, *Elaboratori elettronici e controllo sociale*, cit., p. 92, la tutela risarcitoria risultava successiva e mai pienamente appagante. Per G. Giacobbe, *La responsabilità civile per la gestione di banche dati*, in V. Zeno-Zencovich (a cura di), *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, Jovene, Napoli 1985, p. 93, la tutela della personalità è meglio assicurata mediante rimedi preventivi piuttosto che repressivi. In tema, C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali* e 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., rispettivamente p. 189 ss. e p. 225 ss.

[15] E. Pellecchia, *La responsabilità civile per trattamento dei dati personali*, in *Resp. civ. prev.,* fasc. 2, 2006, p. 226.

Inoltre, sorgeva l'obbligo per il titolare del trattamento di adottare misure idonee e preventive, capaci di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati, nonché di accesso non autorizzato o di trattamento non consentito o difforme rispetto alle finalità della raccolta. Il parametro dell'idoneità, tuttavia, impedì un appiattimento del dovere costante di sicurezza sul parametro di quella minima (art. 15, commi 2 e 3, l. n. 675/1996). L'uniformità rispetto alle misure minime di sicurezza, il cui aggiornamento doveva essere biennale, in ragione degli sviluppi tecnici e logistici, non determinava una neutralizzazione del dovere di adottare ogni misura idonea e preventiva[16]: l'osservanza della prima prescrizione non si traduceva in una area di immunità per il titolare del trattamento rispetto a possibili conseguenze in termini di responsabilità civile o amministrativa derivanti dal mancato ricorso ad ogni misura di sicurezza risultata idonea[17].

Il Codice in materia di protezione dei dati personali, d.lgs. n. 196/2003, posizionò la sicurezza al Titolo V - Sicurezza dei dati e dei sistemi - del compendio normativo: la previsione di un obbligo di sicurezza (art. 31) ricalcò quanto disposto dal previgente art. 15, comma 1, l. n. 675/1996, mentre furono tenute distinte le misure minime di sicurezza, disciplinate dall'art. 33 e dall'Allegato B del Codice[18].

Con l'entrata in vigore del GDPR, si è assistito ad una espansione della sicurezza, riabilitata a principio del trattamento dei dati personali[19]: essa diviene centrale per la tutela dei diritti e delle libertà delle persone fisiche[20], incrementando, quindi, la preservazione della componente

[16] S. Rodotà, *Elaboratori elettronici e controllo sociale*, cit., p. 90; G. Conte. *Diritti dell'interessato e obblighi di sicurezza*, in V. Cuffaro, V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino 1997, p. 264.

[17] S. Sica, Sub *art. 18*, in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla L. 675/1996,* Cedam, Padova 1999, p. 254.

[18] Cfr. G.M. Riccio, Sub *artt. 32-36*, in S. Sica, P. Stanzione (a cura di), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Zanichelli, Bologna 2005, p. 126 ss.; R. Motroni, *La sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Giappichelli, Torino 2007, p. 221 ss.; P. Troiano, Sub *artt. 31-36*, in C.M. Bianca, F.D. Busnelli (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, Cedam, Padova 2007[1] , vol. 1, p. 682 ss.

[19] Sia consentito un rinvio a M. Renna, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, fasc. 4, 2020, p. 1343 ss.

[20] E. Lucchini Guastalla, Privacy e data protection*: principi generali*, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, Giuffrè, Milano 2019, p. 70; A. Mantelero, *La gestione del rischio*, *La protezione dei dati personali in Italia*, in G. Finocchiaro (a cura di), Zanichelli, Bologna 2019, p. 473 ss.

identitaria[21], specialmente nei casi in cui risulti conclamata una situazione di vulnerabilità[22]. In questo contesto, la dimensione del rischio comprova la centralità di una protezione capillare dell'identità soggettiva affidata al concorso di tutele privatistiche e pubblicistiche, di rimedi anticipatori e risarcitori e di obblighi legali di protezione[23]. Risulta necessario un impiego costante di apparati tecnici e organizzativi idonei e aggiornati, capaci di minimizzare i rischi, prima, e la portata degli eventi dannosi, poi, e di fornire una reazione subitanea in caso di violazione dei dati personali[24], ovvero, stando al testo dell'art. 4, n. 12, GDPR, qualora si registri una «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»[25].

Il titolare e il responsabile del trattamento sono tenuti a predisporre dispositivi di sicurezza che garantiscano un costante trattamento conforme al GDPR[26], provvedendo al monitoraggio e al governo del rischio[27]. Ai sensi dell'art. 32, par. 1, GDPR, al fine di assicurare un livello di sicurezza adeguato al rischio, andranno predisposte misure tecniche e organizzative tra cui rientrano: la pseudonimizzazione e la cifratura dei dati personali[28];

[21] Cfr. G. Resta, *Identità personale e identità digitale*, in *Dir. inform.*, fasc. 3, 2007, p. 511 ss.; e, ora, G. Guzzardi, *Il paradigma identitario nella società digitale*, in *Pers. mercato*, fasc. 3, 2023, p. 525 ss.

[22] Cfr. D.J Solove, W. Hartzog, *Breached! Why Data Security Law Fails and How to Improve it*, Oxford University Pres, New York 2022; R. Sloan, R. Warner, *Why Don't We Defend Better? Data Breaches, Risk Management, and Public Policy*, CRC Press, Boca Raton (FL) 2020. *Amplius*, D. Amram, *La transizione digitale delle vulnerabilità e il sistema delle responsabilità*, in *Riv. it. med. leg.*, fasc. 4, 2023, p. 1 ss.

[23] F. Zanovello, *Misure di garanzia e rischio di* data breach *in ambito sanitario*, in A. Thiene, S. Corso (a cura di), *La protezione dei dati sanitari.* Privacy *e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Jovene, Napoli 2023, p. 145 ss.

[24] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 779.

[25] G.M. Riccio, *Data Protection and Appropriate Measures: Too Many Uncertainties in the Judicial Applications?*, in *UNIO - EU Law Journal*, vol. 10(1), 2024, p. 21.

[26] F. Pizzetti, Privacy *e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Giappichelli, Torino 2016², vol. 2, p. 295; A. Mantelero, *La gestione del rischio*, cit., p. 493.

[27] Per alcune considerazioni critiche sul rapporto tra rischio e pericolo, v. S. Sica, Sub *art. 82 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano 2021, p. 894. V., altresì, M. Gambini, *Principio di responsabilità e tutela aquiliana dei dati personali*, Edizioni Scientifiche Italiane, Napoli 2018, p. 92 ss.

[28] G. Giannone Codiglione, Risk-based approach *e trattamento dei dati personali,* in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy,

la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura mediante cui testare, verificare e valutare regolarmente l'efficacia dei dispositivi tecnici e organizzativi. Tuttavia, come recentemente chiarito dal Garante per la protezione dei dati personali, «gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, par. 1, lett. da a) a d), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano»[29]. La valutazione dell'adeguatezza del livello di sicurezza risulterà condizionata anche dal peso attribuito al rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati (art. 32, par. 2, GDPR).

Si fa spazio una visione strategica e globale della sicurezza[30]: la declinazione del principio di sicurezza non tollera una lettura di retroguardia che individui, ancora, nella responsabilità civile il solo strumento di reazione, ma incide e modula in ogni fase - preventiva, operativa e reattiva - l'operato del titolare e del responsabile del trattamento[31]. Come, infatti, si osserva dalla lettura del Considerando 35 GDPR, «una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata».

Wolters Kluwer-Cedam, Assago 2016, p. 67.

[29] Provvedimento del 28 settembre 2023.

[30] G. Resta, *I dati e le informazioni*, in G. Alpa, Id. (a cura di), *Le persone fisiche e i diritti della personalità*, *Le persone e la famiglia*, («Tratt. dir. Civ.»), t. I, diretto da R.Sacco, Utet, Torino 2019, p. 460, insiste sul carattere preventivo che connota il dovere del titolare del trattamento.

[31] Cfr. C. Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Juscivile*, fasc. 3, 2020, p. 791 ss.; A. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Wolters Kluwer-Cedam, Milano 2019, p. 255 ss.

3. *Spunti a partire dal caso VB c. Natsionalna agentsia za prihodite*

Per la prima volta la Corte di giustizia si è pronunciata mediante la sentenza 14 dicembre 2023, causa C-340/21, sull'art. 32 GDPR[32]: la decisione favorisce una riflessione sul principio di sicurezza [art. 5, par. 1, lett. *f*), GDPR], dispositivo giuridico funzionale alla protezione dei dati personali[33]. L'accesso non autorizzato - legato a un attacco *hacker* risalente al 2019 - a numerosi dati conservati dall'Agenzia delle entrate bulgara (titolare del trattamento) aveva condotto il soggetto interessato ad agire per il risarcimento dei danni immateriali, lamentando la violazione dei dati personali[34]. In primo grado, il Tribunale amministrativo della città di Sofia respinse il ricorso in quanto: *i*) trattavasi di un'azione criminosa addebitabile a terzi; *ii*) non era stata sufficientemente provata la correlazione tra l'evento dannoso e l'inerzia del titolare del trattamento circa l'adozione delle appropriate misure di sicurezza; *iii*) difettava il pregiudizio immateriale. Investita del ricorso, la Corte suprema amministrativa sottoponeva alla Corte di giustizia alcune questioni pregiudiziali, legate: 1) all'adeguatezza delle misure di sicurezza e alla responsabilità del titolare del trattamento; 2) all'allocazione dell'onere della prova; 3) alla configurabilità del danno da violazione dei dati personali ai sensi dell'art. 82 GDPR.

I giudici europei hanno chiarito come gli artt. 24 e 32 GDPR impongano al titolare del trattamento l'adozione di misure tecniche e organizzative volte a evitare e, quindi, a contrastare prontamente fenomeni di *data breach*[35]; tale obbligo è correlato ad una valutazione concreta dei

[32] Come osserva l'Avv. Generale Pitruzzella nelle *Conclusioni*, presentate il 27 aprile 2023, trattasi di causa avente ad oggetto questioni parzialmente inedite. Per un primo commento, G.M. Riccio, *Danni non patrimoniali per violazione dei dati personali: verso un'alluvione giudiziaria?*, in *Foro it.*, fasc. 4, 2024, p. 76 ss.; G. Sica, *"Responsabilità" e "danno" da illecito trattamento dei dati personali. Il modello europeo all'indomani del caso VB c. NAP*, in *Dir. Merc. Tec.*, 15 dicembre 2023, p. 1 ss.

[33] F. Bravo, *I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, nel solco delle* rules of construction, in F. Bravo (a cura di), *Dati personali. Protezione, libera circolazione e governance – 1. Principi*, Pacini, Pisa 2023, pp. 48-50. Invero, F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leg. civ. comm.*, vol. 40, fasc. 2, 2017, p. 387, ha interpretato la sicurezza quale specificazione della liceità del trattamento.

[34] La controversia si è incentrata sull'interpretazione e sull'applicazione degli artt. 5, par. 1, lett. *f*), 24, 32 e 82 GDPR.

[35] EPDB, One-Stop-Shop Case Digest on Security of Processing and Data Breach Notification, 18 gennaio 2024.

profili di rischio implicati dal singolo trattamento[36].

La procedimentalizzazione della sicurezza impedisce ricostruzioni astratte o conclusioni assiomatiche[37]: e tanto basterebbe a giustificare una interpretazione contestuale e teleologica. Secondo le parole della Corte, «gli articoli 24 e 32 del RGPD non possono essere intesi nel senso che una divulgazione non autorizzata di dati personali o un accesso non autorizzato a tali dati da parte di un terzo siano sufficienti per concludere che le misure adottate dal titolare del trattamento di cui trattasi non erano appropriate, ai sensi di tali disposizioni, senza neppure consentire a quest'ultimo di fornire la prova contraria»[38]. Inoltre, la sicurezza del trattamento si misura con l'attività di protezione *discrezionale* del titolare legata alla relativa ponderazione di rischi. Non si tratta di arbitrio o di immunità: i singoli giudici nazionali, infatti, nel verificare il rispetto dell'art. 32 GDPR, dovranno compiere una valutazione «della natura e del contenuto delle misure che sono state attuate dal titolare del trattamento, del modo in cui tali misure sono state applicate e dei loro effetti pratici sul livello di sicurezza che quest'ultimo era tenuto a garantire, tenuto conto dei rischi inerenti a tale trattamento»[39].

L'interrogativo sulla distribuzione dell'onere probatorio - e, quindi, più in generale, così come accennato dal Professore Zeno-Zencovich, la c.d. «difficulty of providing evidence of what was actually lost»[40] - viene risolto dai giudici con il richiamo all'*effet utile* regolamentare e alla «responsabilizzazione» che ammanta la condotta del titolare del trattamento: questi, *best risk bearer*[41], sarà tenuto a dimostrare il rispetto delle prescrizioni regolamentari, affinché non sia vanificata l'effettiva tutela delle libertà e dei diritti delle persone fisiche[42]. Dall'altro lato, rimane salvo il potere del singolo giudice nazionale di apprezzare autonomamente, senza astratte preclusioni probatorie, l'adeguatezza delle misure assunte: «una

[36] *Considerando* 76 GDPR. V., ora, Corte giust., 21 dicembre 2023, C-667/21, *ZQ c. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts*, par. 69.

[37] Sulla scorta del *Considerando* 83 GDPR, viene sostenuto come il legislatore abbia «manifestato la sua intenzione di «limitare» i rischi di violazione dei dati personali, senza affermare che sarebbe possibile eliminarli»: par. 38.

[38] Par. 32.

[39] Par. 46. In tema, G.M. Riccio, *Data Protection and Appropriate Measures: Too Many Uncertainties in the Judicial Applications?*, cit., p. 25.

[40] V. Zeno-Zencovich, *Liability for Data Loss*, cit., p. 88.

[41] Il titolare del trattamento è tenuto a registrare le misure di sicurezza approntate [art. 30, par. 1, lett. *g*), GDPR].

[42] Par. 56.

perizia giudiziaria non può costituire un mezzo di prova sistematicamente necessario e sufficiente» (par. 64).

Sul versante difensivo, il titolare del trattamento, per neutralizzare la pretesa risarcitoria avanzata dall'interessato, dovrà dimostrare l'assoluta non imputabilità dell'evento dannoso: non potrà, pertanto, essere invocato l'atto del terzo così da eccepire, *de plano*, l'assenza di qualsivoglia responsabilità[43]. Il danno immateriale, pur sotto forma di timore di un potenziale utilizzo abusivo dei dati personali da parte di terzi a seguito della registrata violazione della sicurezza, dovrà comunque essere debitamente comprovato[44]; al giudice nazionale toccherà il compito di verificare la fondatezza del *petitum*[45]. La Corte - confermando la soluzione elaborata in *UI c. Österreichische Post AG*, ove è contestata la compatibilità di una disposizione statale che assoggetti il risarcimento del danno immateriale al raggiungimento di una predeterminata soglia di gravità del nocumento[46] - ha inteso estendere la portata applicativa dell'art. 82 GDPR, ferma restando l'oggettiva configurabilità del danno[47]: escludere il timore di un utilizzo

[43] Par. 74. Analogamente, «il fatto che alcuni dipendenti del titolare del trattamento abbiano consegnato per errore a un terzo non autorizzato un documento contenente dati personali non è sufficiente, di per sé, a ritenere che le misure tecniche e organizzative attuate dal titolare del trattamento di cui trattasi non fossero "adeguate"», ai sensi degli artt. 24 e 32 GDPR: così, Corte giust., 25 gennaio 2024, C-687/21, *BL c. MediaMarktSaturn Hagen-Iserlohn GmbH*, par. 45.

[44] Da una diversa prospettiva, G. Alpa, *Danno* in re *ipsa e tutela dei diritti fondamentali (diritti della personalità e diritto di proprietà)*, in *Resp. civ. prev.,* vol. 1, 2023, p. 14. Per l'A., «la diffusione non autorizzata e non conforme alla legge di dati personali, o la diffusione di immagini al di fuori dei loro destinatari, o la violazione della *privacy* siano tutti danni apprezzabili *ex se*, e meritevoli di risarcimento».

[45] Parr. 85-86. Come anticipato da C. Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, cit., p. 1157, nt. 41, il danno in questione «ancorché non tale da attingere un livello predeterminato di gravità, deve comunque poter essere oggettivamente apprezzato come tale, anche sulla base di una valutazione social – tipica delle conseguenze, in termini di disagio, suscettibili di derivare dalla violazione del Rgpd».

[46] Per A. Palmieri, R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della* privacy, cit., p. 283, «ciò non vuol dire che l'evocazione di qualsiasi forma di sconcerto/rincrescimento abiliti a ottenere il risarcimento in forza di detto corpo di regole».

[47] *Conclusioni*, cit., parr. 71-74, 77, 82. Appare efficace quanto argomentato nel par. 83: «ciò che conta è che non si tratti di una mera percezione soggettiva, mutevole e dipendente anche da elementi caratteriali e personali, ma la oggettivizzazione di un disagio, seppur lieve ma comprovabile, alla propria sfera fisica o psichica o alla propria vita di relazione; la natura dei dati personali coinvolti e la rilevanza che essi ricoprono nella vita dell'interessato e forse anche la percezione che, in quel momento, abbia la società di quello specifico disagio connesso alla violazione dei dati». S. Pagliantini, *Un altro palcoscenico della «guerra» tra*

abusivo dei dati dal novero dei danni immateriali, secondo il ragionamento della Corte, avrebbe compromesso l'ampiezza «di tale nozione, quale intesa dal legislatore dell'Unione»[48]. Come successivamente precisato dalla Corte di giustizia, «l'articolo 82, paragrafo 1, del RGPD deve essere interpretato nel senso che il timore nutrito da una persona che i suoi dati personali, a causa di una violazione di tale regolamento, siano stati divulgati a terzi, senza che si possa dimostrare che ciò sia effettivamente avvenuto, è sufficiente a fondare un diritto al risarcimento purché tale timore, con le sue conseguenze negative, sia debitamente provato»[49]. La Corte di giustizia, a più riprese, ha poi osservato come la perdita del controllo sui dati - quand'anche occorsa per un breve lasso di tempo - possa integrare un danno causato da una violazione dei dati personali, a condizione che il soggetto interessato «dimostri di aver effettivamente subito un simile danno, per quanto minimo»[50].

4. Data breach*: trasparenza e reazione*

Gli artt. 33 e 34 del GDPR, rispettivamente rubricati «Notifica di una violazione dei dati personali all'autorità di controllo» e «Comunicazione di una violazione dei dati personali all'interessato», verbalizzano una gestione trasparente e condivisa dei fenomeni di *data breach*[51].

Il dovere di notificare di una violazione dei dati personali all'autorità di controllo è posto in capo al titolare del trattamento: pur tuttavia, a riprova della relazionalità che ammanta l'attività del trattamento dei dati personali, il responsabile del trattamento è tenuto ad informare il titolare senza ingiustificato ritardo dopo aver appreso della violazione in essere (art. 33, par. 2, GDPR)[52]. Tale prescrizione notiziale, che conferma la pervasività del

le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr, cit., p. 292, contesta questo approccio: «padrone della scena, così ragionando, diventerà un relativismo sfociante in un ordinamento del caso concreto».

[48] Par. 81.

[49] Corte giust., 20 giugno 2024, C-590/22, *AT e BT c. PS GbR e a.*, par. 36.

[50] Corte giust., 11 aprile 2024, C-741/21, *GP c. juris GmbH*, par. 42

[51] Sul tema, cfr. A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, in *Dir. merc. tec.* , 9 luglio 2018, p. 1 ss. Sia consentito un rinvio a M. Renna, *Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi*, in *Dir. mer. ass. fin.*, 2020, p. 197 ss.

[52] Cfr. S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in S. Sica,

principio di sicurezza e integra un precipitato dell'*accountability approach*[53], non troverà applicazione qualora il titolare del trattamento riesca a dimostrare l'improbabilità di un rischio per i diritti e le libertà delle persone fisiche[54]. Il dovere di notifica di una violazione risulta funzionale alla tutela dell'integrità dei dati e della salvaguardia dei diritti e delle libertà delle persone fisiche ed è fondato sulla procedimentalizzazione della gestione del rischio, nonché modellato in base alla natura e alla gravità della violazione dei dati personali e dei tipi di rischio per l'interessato.

A livello operativo, la notifica andrà effettuata entro 72 ore dalla cognizione del *data breach*: il rispetto della tempistica condurrà, verosimilmente, il titolare del trattamento a dotarsi di una struttura tecnica, di cui è parte anche il responsabile del trattamento, che favorisca un flusso costante di informazioni e che permetta di apprezzare puntualmente le criticità e di valutare con esattezza la natura dei rischi. Ai sensi dell'art. 33, par. 3, GDPR, il titolare dovrà *almeno*:

a) descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

L'obbligo informativo potrà anche essere assolto per fasi: in questo caso, toccherà al titolare del trattamento giustificare le ragioni di una notifica parziale e avviare, contestualmente, un contatto immediato con l'autorità di garanzia. Inoltre, il titolare del trattamento sarà tenuto a documentare le violazioni dei dati personali, nonché i provvedimenti

V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy, cit., p. 8; F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 804.

[53] S. Vigliar, Data breach *e sicurezza informatica*, in S. Sica, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy, cit., p. 245 ss.; E. Maio, Sub *art. 24 GDPR*, in A. Barba, S. Pagliantini (a cura di), *Delle persone*, *Comm. cod. civ.,* vol. 2, diretto da F. Gabrielli, Utet, Milano 2019, p. 503 ss.

[54] La notifica all'autorità di garanzia di una violazione dei dati personali avviene mediante una procedura telematica disponibile al sito <*servizi.gpdp.it*>.

assunti per porvi rimedio[55].

L'art. 34 GDPR enuclea una serie di regole poste a salvaguardia dei diritti del soggetto interessato in caso di violazione dei dati personali: la comunicazione è legata alla stima del livello di rischio. Solo in caso di rischi *elevati* per i diritti e le libertà delle persone fisiche si procederà in tal senso. Attraverso la comunicazione all'interessato, che dovrà essere fornita mediante un linguaggio chiaro e semplice, si devono trasmettere informazioni essenziali circa lo stato dei dati personali trattati, favorendo una tempestiva reazione da parte dell'interessato. Il titolare del trattamento dovrà rendere edotto l'interessato delle informazioni e delle misure, di cui all'art. 33, par. 3, lett. *b*), *c*) e *d*).

Si tratta, nel complesso, di una previsione regolamentare elastica, ma comunque incentrata sull'esigenza di una comunicazione esaustiva e differenziata, là dove ciò risulti necessario al fine della protezione degli interessati[56]. Infatti, ai sensi dell'art. 34, par. 3, GDPR, non si ricorrerà a tale comunicazione qualora sia stato approntato uno dei seguenti rimedi[57]:

a) messa in atto di misure tecniche e organizzative adeguate di protezione e contestuale applicazione ai dati personali oggetto della violazione (vi rientrano, in particolare, quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura);

b) adozione da parte del titolare del trattamento di misure volte a scongiurare il sopravvenire di un rischio elevato per i diritti e le libertà degli interessati;

c) comunicazione pubblica, o in misura equipollente, che consenta una efficace informazione degli interessati nel caso in cui la diretta comunicazione richieda sforzi sproporzionati[58].

[55] G. Finocchiaro, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, Milano 2020, p. 246 s. In tema, v. il Provvedimento del Garante per la protezione dei dati personali del 10 luglio 2025.

[56] Per un'applicazione concreta, v. il Provvedimento del Garante per la protezione dei dati personali del 14 maggio 2020.

[57] A.G. Parisi, *Illiceità del trattamento dei dati personali e rimedi (inibitori, risarcitori, satisfattivi e ablativi)*, in P. Stanzione (a cura di), *I "poteri privati" e le nuove frontiere della privacy*, Giappichelli, Torino 2022, pp. 225-226.

[58] Per un'applicazione concreta, v. il Provvedimento del Garante per la protezione dei dati personali dell'8 giugno 2023; nonché, il Provvedimento del Garante per la protezione dei dati personali del 10 marzo 2022.

5. *Le* Guidelines 9/2022 on personal data breach notification under GDPR

Le linee guida adottate il 28 marzo 2023 aggiornano le precedenti *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250rev.01, del 3 ottobre 2017. L'odierno testo offre una consolidazione di *best practices* in materia di doveri informativi ricadenti sul titolare del trattamento: dalla lettura delle linee guida, emerge la conferma di una visione elastica della sicurezza[59], contestuale e procedimentale, nonché inidonea ad essere *catturata* da schemi rigidi[60]. Il livello di rischio per i diritti e le libertà delle persone fisiche è centrale per l'effettuazione della relativa notifica e ciò si riflette in termini di necessaria e puntuale pianificazione delle fasi attinenti al *data processing*. Vi rientra l'adeguata professionalizzazione dei soggetti coinvolti nel trattamento, al fine di favorire una immediata cognizione e una pronta e proporzionata reazione a seguito del verificarsi di fenomeni di *data breach*.

La notifica risulterà efficace, e come tale funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, qualora sia tempestiva e circostanziata: ciò implica uno scambio di informazioni tra titolare del trattamento, responsabile del medesimo e responsabile della protezione dei dati personali (ove presente). Il responsabile del trattamento, del caso, dovrà comunicare al titolare l'avvenuta violazione dei dati personali senza indebito ritardo, mettendo a disposizione del titolare ogni informazione che risulti utile al fine della decisione di notificare o meno la violazione dei dati personali. Il responsabile della protezione dei dati avrà il dovere di informare il titolare e il responsabile del trattamento e di fornire loro consulenza, oltre a cooperare con l'autorità di controllo e fungere da punto di contatto con riferimento ad ogni questione connessa all'attività del trattamento dei dati.

La notifica potrà essere omessa qualora il titolare del trattamento, dopo aver constatato la consistenza e l'impatto della violazione, reputi *improbabile* una lesione per i diritti e le libertà delle persone fisiche: centrale, ancora una volta, risulta essere l'attività di *risk assessment*[61]. Seguendo le linee guida, dovrà procedersi ad un esame dei rischi collegato

[59] G.M. Riccio, *Data Protection and Appropriate Measures: Too Many Uncertainties in the Judicial Applications?*, cit., pp. 23-24.

[60] M.S. Esposito, Sub *art. 32 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della* privacy *e* data protection, cit., pp. 503-505.

[61] A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, cit., p. 14.

ai seguenti fattori: *a*) tipo di violazione; *b*) natura, carattere sensibile e volume dei dati personali; *c*) facilità di identificazione delle persone; *d*) gravità delle conseguenze per le persone fisiche; *e*) caratteristiche particolari dell'interessato; *f*) caratteristiche particolari del titolare del trattamento di dati; *g*) numero di persone fisiche interessate.

Con riguardo alla comunicazione di un fenomeno di *data breach* all'interessato, le linee guida chiariscono come questo strumento notiziale sia teso alla salvaguardia effettiva dell'interessato in caso di violazioni dei dati personali che presentino rischi *elevati* in termini di diritti e di libertà personali; la comunicazione dovrà essere diretta, chiara e trasparente e soddisfare il requisito di speditezza. Per il titolare del trattamento diviene, nuovamente, essenziale, al fine di non incorrere in responsabilità di marca aquiliana o amministrativa, dotarsi di un apparato di sicurezza efficiente che consenta l'attivazione dei meccanismi di allerta e che favorisca una reazione proporzionata e capace di mitigare le conseguenze dannose derivanti da violazioni della riservatezza ovvero dell'integrità o della disponibilità dei dati[62].

Una preziosa fonte di orientamento per i soggetti coinvolti nel trattamento è costituita dalle linee guida 1/2021 sugli esempi riguardanti la notifica di una violazione dei dati personali, adottate dall'EDPB in data 14 dicembre 2021. Per i casi di *ransomware*, di attacchi di esfiltrazione dei dati, di errore umano, di smarrimento o furto di dispositivi o di documenti cartacei, nonché per errato invio di corrispondenza e altri casi, il *board* europeo offre indicazioni precise e un valido supporto d'ausilio per il titolare del trattamento nella valutazione della violazione dei dati concretamente occorsa. Il documento conferma la necessità di una perdurante responsabilizzazione dei soggetti coinvolti nell'attività di trattamento dei dati, rimarcando la centralità della prevenzione e della minimizzazione dell'impatto del *data breach*. Secondo le linee guida, ogni titolare e ogni responsabile del trattamento dovrebbe disporre di piani e procedure per la gestione di violazioni dei dati, stabilendo un netto riparto dei compiti interno e individuando le figure responsabili delle fasi del processo di recupero[63]. In nome del principio di *accountability* e in

[62] A. Mantelero, *La gestione del rischio*, cit., p. 485 ss.

[63] In tema, con riferimento alla formazione di un *Incident Response Team* e alla redazione di una Matrice RACI, volta a "mettere in relazione le risorse con le attività delle quali sono responsabili, o con le loro aggregazioni", v. G. Vaciago, Sub *art. 33 GDPR*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della* privacy *e* data protection, pp. 518-519. Precisa l'A. che «le risorse vengono distinte in: (i) *Responsible* (colui che esegue ed assegna l'attività); (ii) *Accountable*: è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere

omaggio alla protezione dei dati fin dalla progettazione viene caldeggiata la preparazione di un manuale per la gestione delle violazioni dei dati, predisposto dal titolare e dal responsabile del trattamento.

6. *Considerazioni conclusive*

Il principio di sicurezza rende evidente la necessità di assicurare un trattamento costantemente capace di proteggere i diritti e le libertà fondamentali delle persone fisiche.

Le prescrizioni comunicative addossate in capo al titolare del trattamento in caso di *data breach* si inseriscono in questo scenario e favoriscono l'affermarsi di una tutela anticipatoria:[64] peraltro il rispetto delle procedure informative, quand'anche accompagnato dall'adesione ad un codice di condotta (art. 40, comma 2, lett. *h* e *i*, GDPR) o dotato di una certificazione (art. 42 GDPR), pur non potendo escludere l'eventuale configurarsi di una responsabilità civile in capo al titolare o al responsabile del trattamento, specialmente quando questi omettano di adottare le misure di sicurezza calibrate sui rischi specifici o non aggiornino i dispositivi di sicurezza[65], potrà incidere sulla quantificazione della sanzione amministrativa pecuniaria inflitta ai sensi dell'art. 83, par. 2, lett. *j*), GDPR[66].

univocamente assegnato; (iii) *Consulted* è la persona che aiuta e collabora con il Responsible per l'esecuzione dell'attività; (iv) *Informed* è colui che deve essere informato al momento dell'esecuzione dell'attività» (p. 519).

[64] Chiarisce A. Mantelero, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di* Artificial Intelligence", in Id. e D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa University Press, Pisa 2018, p. 305, che «la sicurezza non è più la mera sicurezza informatica o la sicurezza del processo di trattamento dati, ma è la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali. Solo in questa maniera il primato dell'Unione Europea nel regolare il trattamento dei dati personali potrà rimanere tale, mantenendo fermo un paradigma valoriale, in cui la tutela dei diritti e libertà dei singoli e della collettività prevale su modelli di innovazione dominati dalle dinamiche di mercato».

[65] G.M. Riccio, F. Pezza, *Certification Mechanisms and Liability Rules under the GDPR. When the Harmonisation Becomes Unification*, in A. De Franceschi, R. Schulze (eds.), *Digital Revolution – New Challenges for Law Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, cit., p. 150.

[66] V. *Considerando* 81 GDPR. Si configura una mera presunzione di adeguamento al GDPR che permette un'attenuazione dell'onere della prova in capo al titolare e al responsabile del trattamento, nel caso in cui vengano chiamati a rispondere per danni derivanti dall'attività di trattamento dei dati personali. In tema, D. Poletti, M.C.

Dalla lettura degli artt. 32, 33 e 34 GDPR emerge il delinearsi di un autonomo diritto degli interessati a un trattamento sicuro che conforma in ogni fase l'attività di *data processing*. La predisposizione di meccanismi di sicurezza sempre adeguati e idonei diviene, allora, per il titolare del trattamento un *asset* strategico[67] e ciò richiama l'opportunità di far ricorso ad appositi meccanismi assicurativi[68] che si rivelino capaci di assorbire le esternalità negative derivanti da un'eventuale responsabilità per danni causalmente connessi alla violazione delle previsioni regolamentari in materia di sicurezza[69], senza che ciò intacchi il regime di responsabilità amministrativa delineato dall'art. 83 GDPR[70]. Come, infatti, ha osservato il Professore Zeno-Zencovich, nel saggio più volte menzionato, «ordinary judicial remedies (both contractual and noncontractual) are quite ineffective also because of the very high administrative and legal costs. Much more efficient – *de lege ferenda* – is a system in which compulsory insurance for data service providers is supplemented by simplified and semi-automatic compensation procedures, similar – although on a larger scale – to those one already finds in the EU transport law for the protection of passengers»(pp. 90-91).

Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy, cit., p. 379.

[67] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 782. Ora, L. Miotto, *Organizzazione d'impresa e gestione dei dati personali. Il rischio di* non compliance *nelle catene di fornitura*, Giappichelli, Torino 2023, spec. p. 44 ss.

[68] V. il documento redatto da IVASS, *Indagine sulle polizze a copertura del* cyber risk, ottobre 2023.

[69] Con riferimento al rapporto tra *accountability* e responsabilità civile, chiarisce G. Comandè, *Lettera sulla responsabilità (civile) e l'autonomia (individuale)*, in *Danno e responsabilità*, 2022, p. 668: «così sono i meccanismi e le prassi caratteristici dell'attività e largamente lasciati all'autonomia del singolo a divenire parametro per verificare se le scelte di autonomia organizzativa per prevenire o per come reagire a un *data breach* conducano o meno a responsabilità o si fermino a rendicontare tempestivamente le azioni a tutela poste in essere, per esempio. In tal modo, anche la causazione di un danno non porta automaticamente a risarcirlo se si sono rispettati i parametri e le modalità comportamentali previste dal sistema; viceversa, anche la mancata causazione di un danno risarcibile può portare ad una "sanzione" per la "mera" violazione della *accountability*». In tema, A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, cit., p. 26 ss.

[70] F. Mezzanotte, *L'allocazione convenzionale del rischio «da illecito» (con particolare riguardo alle sanzioni amministrative pecuniarie)*, in *Riv. dir. civ.*, fasc. 3, 2010, p. 203 ss. Cfr., altresì, S. Landini, *Assicurazione e responsabilità*, Giuffrè, Milano 2004, pp. 343 ss.; C.F. Giampaolino, *Le assicurazioni. L'impresa - I contratti*, («Tratt. dir. comm.»), t. III, fondato da V. Buonocore, Giappichelli, Torino 2013, p. 182 ss.