LA DISCIPLINA DEL *DATA BREACH* NEL GDPR: NOTE SU VIOLAZIONE DEI DATI PERSONALI E SICUREZZA DEL TRATTAMENTO

PERSONAL DATA BREACH AND SECURITY OF PROCESSING IN GDPR

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 992-1007

Mario RENNA

ARTICOLO CONSEGNATO: 13 de octubre de 2022
ARTICOLO APPROBATO: 5 de diciembre de 2022

ABSTRACT: Ai sensi del GDPR, il trattamento dei dati personali dovrà risultare conforme al principio di sicurezza. Ciò costituisce un incremento del livello di tutela dei soggetti interessati e al, contempo, impone al titolare del trattamento e al responsabile una costante e aggiornata valutazione dei profili di rischio. Lo scritto si sofferma sulla notifica all'autorità di garanzia e sulla comunicazione all'interessato aventi ad oggetto la violazione dei dati personali.

PAROLE CHIAVE: Violazione dei dati personali; GDPR; Principio di sicurezza; Trasparenza.

ABSTRACT: *The processing of personal data must respect the principle of security. The GDPR shows an increase in the level of protection of the data subjects; at the same time, the accountability approach obliges the data controller and the processor to carry out a constant and updated assessment of the risk profiles. The paper also focuses on the notification to the supervisory authority and on the communication to the data subject of a personal data breach.*

KEY WORDS: *Data breach; GDPR; Security; Notification.*

SOMMARIO.- I. PRINCIPIO DI SICUREZZA E VIOLAZIONE DEI DATI PERSONALI. – II. IL CONTRASTO TRASPARENTE AL DATA BREACH. – III. DATA BREACH NOTIFICATION: SPUNTI DALLE LINEE GUIDA EUROPEE – IV. CONSIDERAZIONI CONCLUSIVE.

I. PRINCIPIO DI SICUREZZA E VIOLAZIONE DEI DATI PERSONALI.

Il GDPR - Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – colloca la sicurezza tra i principi applicabili al trattamento dei dati personali[1]: più precisamente, i dati personali devono essere trattati in modo da garantire una adeguata sicurezza e una costante integrità e riservatezza (art. 5, par. 1, lett. *f*). Tale configurazione giuridica incentiva un esame relazionale e contestuale delle responsabilità gravanti sul titolare e sul responsabile del trattamento, per i quali si impone una valutazione costante e prudente dei rischi: per costoro, con riferimento ad ogni fase dell'attività del trattamento dei dati, si configura un dovere di prevenzione, di mantenimento di un livello di sicurezza adeguato ai rischi e di tempestiva reazione a seguito di violazioni della sicurezza, discendendo da ciò un incremento del livello di protezione dei diritti e delle libertà delle persone fisiche e, quindi, dei soggetti interessati[2].

Giova ricordare come la sicurezza abbia costituito, sin dalla Convenzione di Strasburgo n. 108/81 «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», un fattore centrale nell'attività del trattamento dei dati[3], assurgendo al rango di principio fondamentale, come tale inderogabile[4]. Secondo il 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

1 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

2 Cfr. Mantelero A., Vaciago G.: "Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector", in *Privacy and Data Protection in Software Services* (a cura di R. Senigaglia, C. Irti, A. Bernes), Springer (eBook), 2022, pp. 97 ss.; Sica T.: "Cybersecurity and risk management", *Corporate governance*, 2022, pp. 581 ss.; Laghi P.: "Struttura della rete e responsabilità: *cybersecurity*", in AA. VV.: *Rapporti civilistici e intelligenze artificiali: attività e responsabilità. Atti del 15° convegno nazionale (SISDiC)*, Esi, Napoli, 2020, pp. 255 ss.; Tosi E.: *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.

3 Rodotà S.: *Elaboratori elettronici e controllo sociale*, il Mulino, Bologna, 1973, pp. 81 ss.; Id.: "Protezione dei dati e circolazione delle informazioni", in Id., *Tecnologie e diritti*, il Mulino, Bologna, 1995, pp. 41 ss.; Frosini V.: "*Diritto alla riservatezza e calcolatori elettronici*", in *Banche dati, telematica e diritti della persona* (a cura di G. Alpa, M. Bessone), Cedam, Padova, 1984, pp. 29 ss.; Corasaniti G.: *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003; *Tutela della privacy e misure di sicurezza dei dati personali* (a cura di F. Casucci), Esi, Napoli, 2006.

4 Rodotà S.: "Tecnologie dell'informazione e frontiere del sistema socio-politico", in *Banche dati, telematica e diritti della persona*, cit., pp. 89 ss., 94.

• Mario Renna
Ricercatore nell'Università di Siena
mario.renna@unisi.it

autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate». Anche a seguito delle 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 in termini di principio ordinatore[5].

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[6], non si allineò alla Convenzione di Strasburgo, in quanto la sicurezza venne derubricata a mera regola di condotta, il cui rispetto gravava esclusivamente sul responsabile del trattamento (art. 17)[7]. 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 implicante trasmissioni di dati in rete.

Nel testo della l. n. 675/1996, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, la sicurezza non comparve né tra le finalità della normativa né rappresentò un principio per il trattamento dei dati; non si intese assegnare all'interessato un diritto ad ottenere una tutela anticipatoria, venendo individuato nel solo rimedio risarcitorio lo strumento per ricomporre le perdite patite a seguito della violazione della disciplina della sicurezza[8].

L'adozione di misure di sicurezza era legata allo stato di conoscenze acquisite in base al progresso tecnico[9]: la custodia e il controllo dei dati dovevano essere calibrati rispetto alla natura dei dati medesimi e alle specifiche caratteristiche del trattamento. Inoltre, sorgeva l'obbligo per il titolare del trattamento di adottare misure idonee e preventive, che riducessero ogni rischio di distruzione o perdita,

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

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

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

8 Secondo Rodotà S.: *Elaboratori elettronici e controllo sociale*, cit., p. 92, la tutela risarcitoria risulta(va) successiva e mai pienamente appagante. Per Giacobbe G.: "La responsabilità civile per la gestione di banche dati", in *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione* (a cura di V. Zeno-Zencovich), Jovene, Napoli, 1985, p. 93, la tutela della personalità risulta(va) meglio assicurata mediante rimedi preventivi piuttosto che repressivi. In tema, Castronovo C.: "Situazioni soggettive e tutela nella legge sul trattamento dei dati personali" e di Majo A.: "Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela", entrambi in *Trattamento dei dati e tutela della persona*, cit., rispettivamente pp. 189 ss. e 225 ss.

9 Pellecchia E.: "La responsabilità civile per trattamento dei dati personali", *Resp. civ. prev.,* 2006, p. 226.

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 impedì l'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 considerazione degli sviluppi tecnici e logistici – non depotenziava, dunque, il dovere di adottare le misure idonee e preventive[10]: l'osservanza della prima prescrizione non poteva condurre ad una immunità per il titolare del trattamento rispetto a possibili conseguenze in termini di responsabilità aquiliana o amministrativa derivanti dal mancato ricorso ad ogni misura di sicurezza risultata idonea[11].

Il Codice in materia di protezione dei dati personali, d.lgs. n. 196/2003, "relegò" la sicurezza al Titolo V «Sicurezza dei dati e dei sistemi»: la previsione di un obbligo di sicurezza (art. 31 Codice) 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[12].

Il GDPR, alterando la tendenza positiva alla *compressione* del portato della sicurezza, assegna a quest'ultima il ruolo di principio del trattamento dei dati personali[13], al fine di incrementare l'ampiezza della tutela dei diritti e delle libertà delle persone fisiche[14]. Si impone la necessità di un impiego costante di apparati tecnici e organizzativi idonei e aggiornati, capaci di minimizzare i rischi e di fornire una reazione subitanea in caso di violazione dei dati personali[15], ovvero, stando al testo dell'art. 4, n. 12, GDPR, di ogni "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".

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

11 Sica S.: "Art. 18", in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich, *La tutela dei dati personali. Commento alla L. 675/1996*, Cedam, Padova, 1999, p. 254.

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

13 Sia consentito un rinvio a Renna M.: "Sicurezza e gestione del rischio nel trattamento dei dati personali", *Resp. civ. prev.*, 2020, pp. 1343 ss.

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

15 Bravo F.: "L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi", cit., p. 779.

Spetta al titolare e al responsabile del trattamento la predisposizione di dispositivi di sicurezza che garantiscano un trattamento conforme al GDPR[16]: più precisamente, l'operato dei predetti soggetti risulterà inciso dalla dinamica del fattore rischio[17]. A mente 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[18]; 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[19].

Infine, la valutazione dell'adeguatezza del livello di sicurezza risulterà condizionata, anche, dal peso assegnato 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)[20]. Dal quadro regolamentare, oltre al deciso processo di *accountability* che contamina l'attività del titolare e del responsabile del trattamento, si fa spazio una visione strategica della sicurezza[21]: la declinazione del principio di sicurezza non tollera una lettura di retroguardia che individui, ancora, nella responsabilità civile il solo strumento di reazione, ma conforma e modula in ogni fase – preventiva, operativa e reattiva - l'operato del titolare e del responsabile del trattamento[22].

16 Pizzetti F.: Privacy e *il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Giappichelli, Torino, 2016, p. 295; Mantelero A.: "La gestione del rischio", cit., p. 493.

17 Per alcune considerazioni critiche sul rapporto tra rischio e pericolo, v. Sica S.: "Art. 82 GDPR", in *Codice della* privacy e data protection (a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta), Giuffrè, Milano, 2021, p. 894. Secondo l'A. "nel tempo presente vi è la tendenza ad abbandonare la nozione di pericolo, che è propria delle società prescientiste, per quella di rischio, che sottende la standardizzazione e la prevedibilità assoluta […]. Ma nel caso del trattamento dei dati personali c'è il pericolo, non il rischio. Da ciò deriva la convinzione della necessità di regole di responsabilità il più possibile orientate verso la tutela della vittima, esposta a un pericolo e non a un rischio prevedibile tout court: l'"imprevedibile" è sempre dietro l'angolo e non può che farsene carico chi trae vantaggio dall'attività pericolosa". V., altresì, Gambini M.: *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, Napoli, 2018, pp. 92 ss.

18 Giannone Codiglione G.: "*Risk-based approach* e trattamento dei dati personali", in *La nuova disciplina europea della* privacy (a cura di S. Sica, V. D'Antonio, G.M. Riccio), Wolters Kluwer-Cedam, Assago, 2016, p. 67.

19 Fonderico G.: "La regolazione amministrativa del trattamento dei dati personali", *Giorn. dir. amm*., 2018, p. 420.

20 In tema, cfr. Hladjk J.: "Art. 32", in *Datenschutz-Grundverordnung* (a cura di E. Ehmann, M. Selmayr), Beck-LexisNexis, München, 2018, p. 517 s.; Piltz C.: "Art. 32", in *DS-GVO. Kommentar* (a cura di P. Gola, D. Heckmann), Beck, München, 2022, pp. 664 ss.

21 Resta G.: "I dati e le informazioni", in G. Alpa, Id., *Le persone fisiche* e *i diritti della personalità*, in *Tratt. Sacco*, Utet, Torino, 2019, p. 460, insiste sul carattere preventivo che connota il dovere del titolare del trattamento.

22 Cfr.: Camardi C.: "Note critiche in tema di danno da illecito trattamento dei dati personali", *Jus Civile*, 2020, spec. p. 791 ss.; Mollo A.: "Gli obblighi previsti in funzione di protezione dei dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi Galgano), Wolters Kluwer-Cedam, Milano, 2019, pp. 255 ss.

II. IL CONTRASTO TRASPARENTE AL *DATA BREACH*.

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", codificano una gestione trasparente e condivisa dei fenomeni di *data breach*[23].

Il dovere di notificare di una violazione dei dati personali all'autorità di controllo è posto in capo al titolare del trattamento: la posizione del primo non è isolata, in quanto il responsabile del trattamento, in questo contesto, è tenuto ad informare il titolare senza ingiustificato ritardo dopo aver appreso della violazione (art. 33, comma 2, GDPR)[24]. Tale prescrizione notiziale, manifestazione della pervasività del principio di sicurezza e precipitato dell'*accountability approach*[25], 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[26]. Complessivamente, il dovere di notifica di una violazione, funzionale alla tutela dell'integrità dei dati e della salvaguardia dei diritti e delle libertà delle persone fisiche, risulta essere fondato sulla procedimentalizzazione della gestione del rischio e modellato in base alla natura e alla gravità della violazione dei dati personali, nonché dei tipi di rischio per l'interessato[27].

A livello operativo, la notifica andrà effettuata entro settantadue ore dal momento in cui il titolare è avvenuto a conoscenza del *data breach*[28]: il rispetto di una stretta tempistica condurrà il titolare del trattamento a dotarsi di una struttura tecnica, di cui è parte anche il responsabile del trattamento, che agevoli un flusso costante di informazioni e che consenta di valutare con esattezza la natura dei rischi[29]. A mente 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

23 Sia consentito un rinvio a Renna M.: "Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi", *Dir. merc. ass. e fin.*, 2020, pp. 197 ss.

24 Cfr. Sica S.: "Verso l'unificazione del diritto europeo alla tutela dei dati personali?", in *La nuova disciplina europea della* privacy, cit., p. 8; Bravo F.: "L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi", cit., p. 804.

25 Vigliar S.: "*Data breach* e sicurezza informatica", in *La nuova disciplina europea della* privacy, cit., pp. 245 ss.; Maio E.: "Art. 24 GDPR", in *Delle persone* (a cura di A. Barba, S. Pagliantini), II, in *Comm. Gabrielli*, Utet, Milano, 2019, pp. 503 ss.

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

27 Pizzetti F.: Privacy e *il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Giappichelli, Torino, 2016, p. 291, nt. 54.

28 Voigt P., von dem Bussche A.: *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer (eBook), 2017, pp. 65 ss.

29 Burton C.: "Art. 33", in AA. VV.: *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, Oxford University Press, 2020, pp. 640 ss.

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 da parte del titolare del trattamento 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: il titolare del trattamento comunicherà i soli dati in suo possesso, giustificando le ragioni della notifica parziale e avviando un contatto immediato con l'autorità di garanzia. Inoltre, il titolare del trattamento documenterà le violazioni dei dati personali, nonché i provvedimenti assunti per porvi rimedio[30].

L'art. 34 GDPR scandisce un plesso di regole posto a salvaguardia dei diritti del diretto interessato in caso di violazione dei dati personali: la comunicazione è connessa alla stima del livello di rischio, poiché avverrà solo in caso di rischi elevati per i diritti e le libertà delle persone fisiche[31]. La comunicazione all'interessato, che dovrà essere fornita mediante un linguaggio chiaro e semplice, permetterà di veicolare una essenziale comunicazione 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. Ai sensi dell'art. 34, par. 3, GDPR, non si ricorrerà a tale comunicazione qualora sia stato approntato uno dei seguenti rimedi satisfattivi[32]:

a) messa in atto delle misure tecniche e organizzative adeguate di protezione e relativa applicazione ai dati personali oggetto della violazione, tra cui in particolare vi rientrano 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;

30 Finocchiaro G.: "Riflessioni su intelligenza artificiale e protezione dei dati personali", in *Intelligenza artificiale. Il diritto, i diritti, l'etica* (a cura di U. Ruffolo), Giuffrè, Milano, 2020, p. 246 s.

31 Zeno-Zencovich V.: "Liability for data loss", in *Research Handbook in Data Science and Law* (a cura di V. Mak, E.Tjong Tjin Tai, A. Berlee), Edward Elgar Publishing, Cheltenham, 2018, p. 51.

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

c) comunicazione pubblica o misura equipollente che informi efficacemente gli interessati nel caso in cui la diretta comunicazione richieda sforzi sproporzionati.

III. *DATA BREACH NOTIFICATION*: SPUNTI DALLE LINEE GUIDA EUROPEE.

Le linee guida *WP250* - adottate il 3 ottobre 2017, e successivamente emendate per mezzo della versione del 6 febbraio 2018, dal "Gruppo di lavoro Articolo 29" - intervengono sulla notifica e sulla comunicazione delle violazioni dei dati personali ai sensi del GDPR. Dal testo delle *best practices* in materia di doveri informativi ricadenti sul titolare del trattamento emerge una visione elastica della sicurezza, insofferente ad essere ingabbiata entro schemi predefiniti e non suscettibili di condizionamenti contestuali[33]; il livello di rischio per i diritti e le libertà delle persone fisiche, come si è visto, centrale per l'effettuazione della notifica, comprova la necessità di una pianificazione capillare delle fasi del *data processing*, tra cui rientra una opportuna professionalizzazione dei soggetti coinvolti nel trattamento, al fine di favorire una immediata cognizione e una pronta e proporzionata reazione a seguito di fenomeni di *data breach*.

La notifica risulterà più efficace, e quindi rappresenterà uno strumento funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, qualora sia tempestiva e circostanziata (il che sottende uno scambio di informazioni tra titolare del trattamento, responsabile del medesimo e responsabile della protezione dei dati personali che sia costante e aggiornato). Come si evince dal testo in rassegna: *i*) il responsabile del trattamento 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; *ii*) il responsabile della protezione dei dati, ove presente, ha il dovere di informare il titolare del trattamento e il responsabile 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 nel caso in cui il titolare del trattamento, verificati consistenza e 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*[34]. Seguendo le linee guida, dovrà procedersi ad un esame dei rischi collegato ai seguenti fattori: *a*) tipo di violazione; *b*) natura, carattere sensibile e volume dei dati personali; *c*) facilità di identificazione delle

33 Esposito M.S.: "Art. 32 GDPR", in *Codice della* privacy e data protection, cit., pp. 503-505.

34 Si riporta il testo del *Considerando* 76 GDPR: "la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato".

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 riferimento all'art. 34 GDPR, le linee guida chiariscono come la comunicazione ambisca a rappresentare uno strumento di 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 prontezza temporale. Soprattutto per il titolare del trattamento diviene, ancora una volta, opportuno, 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 ancora della disponibilità dei dati[35].

Una preziosa fonte di orientamento per i soggetti coinvolti nel trattamento è costituita dalle linee guida 1/2021 su 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 (*social engineering*), il *board* europeo offre indicazioni precise e un valido supporto d'ausilio per il titolare del trattamento nella valutazione dei dati concretamente occorsa. Il documento conferma, infine, 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*. Più concretamente, secondo le linee guida, ogni titolare e responsabile del trattamento dovrebbero 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[36]. In nome del principio di *accountability* e in 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.

35 Mantelero A.: "La gestione del rischio", cit., p. 485 ss.

36 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. Vaciago G.: "Art. 33 GDPR", in *Codice della* privacy e data protection, cit., 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 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).

IV. CONSIDERAZIONI CONCLUSIVE.

Il principio di sicurezza rende evidente la necessità di assicurare un trattamento costantemente al riparo da violazioni di dati personali che possano pregiudicare i diritti e le libertà fondamentali delle persone fisiche[37]: al contempo, le prescrizioni comunicative addossate in capo al titolare del trattamento sono volte a garantire effettività alla salvaguardia della personalità degli interessati e, più in generale, delle persone fisiche potenzialmente vittime di *data breach*[38]. Il principio di sicurezza, come declinato dagli artt. 32, 33 e 34 GDPR, (i) favorisce l'emergere di un autonomo diritto degli interessati a un trattamento governato dalla prevenzione e dalla minimizzazione delle conseguenze dannose; (ii) incide fortemente sull'attività di *data processing*. La predisposizione di meccanismi di sicurezza sempre adeguati e idonei diviene, allora, per il titolare del trattamento un *asset* strategico[39], anche al fine di prevenire ed escludere l'insorgere di responsabilità per danni materiali o immateriali causati dalla violazione delle previsioni regolamentari in materia di sicurezza (così come previsto dall'art. 82 GDPR) o di impedire e contenere l'irrogazione di sanzioni amministrative pecuniarie (alla luce di quanto disposto dall'art. 83 GDPR)[40].

37 Sui diritti dell'interessato disciplinati dal GDPR, cfr. Piraino F.: "I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali", *Giur. it.,* 2019, p. 2789 ss.; Di Lorenzo G.: "Spunti di riflessione su taluni «diritti dell'interessato»", in *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 237 ss.

38 Chiarisce Mantelero A.: "La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di *Artificial Intelligence*", in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (a cura di Id., D. Poletti), Pisa University Press (eBook), 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».

39 Bravo F.: "*L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi",* cit., p. 782. Ora, Miotto L.: *Organizzazione d'impresa e gestione dei dati personali. Il rischio di* non compliance *nelle catene di fornitura*, Giappichelli, Torino, 2023, spec. p. 1 ss., 44 ss.

40 Con riferimento al rapporto tra *accountability* e responsabilità civile, chiarisce Comandè G.: "Lettera sulla responsabilità (civile) e l'autonomia (individuale)", *Danno e resp.*, 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*".

BIBLIOGRAFIA

AA. VV.: *Tutela della privacy e misure di sicurezza dei dati personali* (a cura di F. Casucci), Esi, Napoli, 2006.

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

Burton C.: "Art. 33", in AA. VV.: *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, Oxford University Press, 2020.

Camardi C.: "Note critiche in tema di danno da illecito trattamento dei dati personali", *Jus Civile*, 2020.

Castronovo C.: "Situazioni soggettive e tutela nella legge sul trattamento dei dati personali", in *Trattamento dei dati e tutela della persona* (a cura di V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich), Giuffrè, Milano, 1998.

Comandè G.: "Lettera sulla responsabilità (civile) e l'autonomia (individuale)", *Danno e resp.*, 2022.

Conte G.: "Diritti dell'interessato e obblighi di sicurezza", in *La disciplina del trattamento dei dati personali* (a cura di V. Cuffaro, V. Ricciuto), Giappichelli, Torino, 1997.

Corasaniti G.: *Esperienza giuridica e sicurezza informatica*, Giuffrè, Milano, 2003.

di Majo A.: "Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela", in *Trattamento dei dati e tutela della persona* (a cura di V. Cuffaro, V. Ricciuto, V. Zeno-Zencovich), Giuffrè, Milano, 1998.

Di Lorenzo G.: "Spunti di riflessione su taluni «diritti dell'interessato»", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi Galgano), Wolters Kluwer-Cedam, Milano, 2019.

Esposito M.S.: "Art. 32 GDPR", in *Codice della* privacy e data protection (a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta), Giuffrè, Milano, 2021.

Finocchiaro G.: "Riflessioni su intelligenza artificiale e protezione dei dati personali", in *Intelligenza artificiale. Il diritto, i diritti, l'etica* (a cura di U. Ruffolo), Giuffrè, Milano, 2020.

Fonderico G.: "La regolazione amministrativa del trattamento dei dati personali", *Giorn. dir. amm.*, 2018.

Frosini V.: "*Diritto alla riservatezza e calcolatori elettronici*", in *Banche dati, telematica e diritti della persona* (a cura di G. Alpa, M. Bessone), Cedam, Padova, 1984.

Gambini M.: *Principio di responsabilità e tutela aquiliana dei dati personali*, Esi, Napoli, 2018.

Giacobbe G.: "La responsabilità civile per la gestione di banche dati", in *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione* (a cura di V. Zeno-Zencovich), Jovene, Napoli, 1985.

Giannone Codiglione G.: "*Risk-based approach* e trattamento dei dati personali", in *La nuova disciplina europea della* privacy (a cura di S. Sica, V. D'Antonio, G.M. Riccio), Wolters Kluwer-Cedam, Assago, 2016.

Hladjk J.: "Art. 32", in *Datenschutz-Grundverordnung* (a cura di E. Ehmann, M. Selmayr), Beck-LexisNexis, München, 2018.

Laghi P.: "Struttura della rete e responsabilità: *cybersecurity*", in AA. VV.: *Rapporti civilistici e intelligenze artificiali: attività e responsabilità. Atti del 15° convegno nazionale (SISDiC)*, Esi, Napoli, 2020.

Lucchini Guastalla E.: "*Privacy* e *data protection*: principi generali", in Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice* Privacy (a cura di E. Tosi), Giuffrè, Milano, 2019.

Maio E.: "Art. 24 GDPR", in *Delle persone* (a cura di A. Barba, S. Pagliantini), II, in *Comm. Gabrielli*, Utet, Milano, 2019.

Mantelero A.: "La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di *Artificial Intelligence*", in *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna* (a cura di Id., D. Poletti), Pisa University Press (eBook), 2018.

Mantelero A.: "La gestione del rischio", in *La protezione dei dati personali in Italia* (opera diretta da G. Finocchiaro), Zanichelli, Bologna, 2019.

Mantelero A., Vaciago G.: "Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector", in *Privacy and Data Protection in Software Services* (a cura di R. Senigaglia, C. Irti, A. Bernes), Springer (eBook), 2022.

Miotto L.: *Organizzazione d'impresa e gestione dei dati personali. Il rischio di* non compliance *nelle catene di fornitura*, Giappichelli, Torino, 2023.

Mollo A.: "Gli obblighi previsti in funzione di protezione dei dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi Galgano), Wolters Kluwer-Cedam, Milano, 2019.

Motroni R.: "La sicurezza dei dati e dei sistemi", in *Il Codice del trattamento dei dati personali* (a cura di V. Cuffaro, R. D'Orazio, v. Ricciuto), Giappichelli, Torino, 2007.

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

Pellecchia E.: "La responsabilità civile per trattamento dei dati personali", *Resp. civ. prev.,* 2006.

Piltz C.: "Art. 32", in *DS-GVO. Kommentar* (a cura di P. Gola, D. Heckmann), Beck, München, 2022.

Piraino F.: "I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali", *Giur. it.,* 2019.

Pizzetti F.: Privacy e *il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Giappichelli, Torino, 2016.

Pizzetti F.: Privacy e *il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Giappichelli, Torino, 2016.

Renna M.: "Sicurezza e gestione del rischio nel trattamento dei dati personali", *Resp. civ. prev.*, 2020.

Renna M.: "Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi", *Dir. merc. ass.* e *fin.*, 2020.

Resta G.: "I dati e le informazioni", in G. Alpa, Id., *Le persone fisiche* e *i diritti della personalità*, in *Tratt. Sacco*, Utet, Torino, 2019.

Riccio G.M.: "Artt. 32-36", in *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196* (a cura di S. Sica, P. Stanzione), Zanichelli, Bologna, 2005.

Rodotà S.: *Elaboratori elettronici* e *controllo sociale*, il Mulino, Bologna, 1973.

Rodotà: "Protezione dei dati e circolazione delle informazioni", in Id., *Tecnologie e diritti*, il Mulino, Bologna, 1995.

Sica S.: "Art. 18", in E. Giannantonio, M.G. Losano, V. Zeno-Zencovich, *La tutela dei dati personali. Commento alla L. 675/1996*, Cedam, Padova, 1999.

Sica S.: "Verso l'unificazione del diritto europeo alla tutela dei dati personali?", in *La nuova disciplina europea della* privacy (a cura di Id., V. D'Antonio, G.M. Riccio), Wolters Kluwer-Cedam, Assago, 2016.

Sica S.: "Art. 82 GDPR", in *Codice della* privacy e data protection (a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta), Giuffrè, Milano, 2021.

Sica T.: "Cybersecurity and risk management", *Corporate governance*, 2022.

Tosi E.: *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.

Troiano P.: "Artt. 31-36", in *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)* (a cura di C.M. Bianca, F.D. Busnelli), I, Cedam, Padova, 2007.

Vaciago G.: "Art. 33 GDPR", in *Codice della* privacy e data protection (a cura di R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta), Giuffrè, Milano, 2021.

Vigliar S.: "*Data breach* e sicurezza informatica", in *La nuova disciplina europea della* privacy (a cura di S. Sica, V. D'Antonio, G.M. Riccio), Wolters Kluwer-Cedam, Assago, 2016.

Voigt P., von dem Bussche A.: *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer (eBook), 2017.

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

Zeno-Zencovich V.: "Liability for data loss", in *Research Handbook in Data Science and Law* (a cura di V. Mak, E.Tjong Tjin Tai, A. Berlee), Edward Elgar Publishing, Cheltenham, 2018.