IANUS
Diritto e Finanza

UNIVERSITÀ DI SIENA
1240

Rivista di studi giuridici

https://www.rivistaianus.it

ISSN: 1974-9805

n. 22 - dicembre 2020

APPUNTI SULLA SICUREZZA NEL TRATTAMENTO DEI DATI E *DATA BREACH*

Federico Bianca

APPUNTI SULLA SICUREZZA NEL TRATTAMENTO DEI DATI E *DATA BREACH* °

Federico Bianca

Avvocato del Foro di Roma

Il saggio si propone di esaminare se le norme del Reg. UE 679/16 in materia di sicurezza del trattamento dei dati personali appaiono adeguate nel caso di data breach e se il bilanciamento degli interessi presi in considerazione dal Regolamento (tutela della libertà e dignità delle persone da un lato e sviluppo dell'economia digitale dall'altro) sia assicurato anche mediante i meccanismi di individuazione della responsabilità in caso di mancato trattamento sicuro dei dati e di individuazione dei criteri risarcitori.

The purpose of this essay is to examine whether the rules of EU Reg. 679/16 on the security of personal data processing appear adequate in the event of a data breach and whether the balance of interests taken into account by the Regulation (protection of the freedom and dignity of individuals on the one hand and development of the digital economy on the other) is also ensured through the mechanisms for identifying liability in the event of failure to process data securely and for identifying the criteria for compensation.

Sommario:

° Double blind peer-reviewed paper.

1. Indicazione delle norme del GDPR sulla sicurezza nel trattamento dei dati

Gli artt. 32, 33 e 34 del GDPR contengono le norme relative all'obbligo del titolare del trattamento di garantire la sicurezza del trattamento dei dati e di svolgere una serie di attività nel caso in cui si verifichi la violazione dei dati.

Queste norme fissano il principio per cui gli adempienti (misure tecniche ed organizzative) messi in atto dal titolare del trattamento devono garantire un livello di sicurezza adeguato al rischio inerente lo specifico trattamento dei dati.

Oltre all'adozione di specifiche attività – come l'uso di pseudonimi o la cifratura dei dati; la capacità di assicurare *su base permanente* la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristino e la messa a punto di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche adottate al fine di garantire la sicurezza del trattamento – oltre a tutti questi adempimenti, dicevamo, appare fondamentale la valutazione preliminare e generale del rischio presentato dal trattamento.

Questi principi fissati dall'art. 32 devono poi essere letti in combinato con gli adempimenti previsti dagli artt. 33 e 34 nel caso in cui avvenga una violazione dei dati personali perché in questo caso scattano dei precisi obblighi informativi che hanno lo scopo da un lato di mettere in condizioni l'autorità di controllo di verificare (a posteriori) l'adeguatezza delle misure messe in atto per evitare la violazione (c.d. *data breach*) e dall'altro di consentire all'interessato (proprietario dei dati) di valutare eventuali danni a suo carico.

La dottrina ha correttamente messo in risalto che il GDPR ha attribuito alla sicurezza il valore di principio fondamentale informatore del trattamenti dei dati personali, privilegiandone il carattere funzionale ed assegnandone un valore elastico (art. 5, lett. f GDPR)[1].

2. L'approccio basato sulla preventiva valutazione del rischio

Questa impostazione sottolinea la rilevanza che il GDPR attribuisce al c.d. *risk-based approach* ed alla responsabilizzazione o *accountability* del titolare del trattamento[2].

---

[1] RENNA, *Sicurezza dei dati personali*, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 627.

[2] BATTELLI, *La valutazione d'impatto introdotta dal GDPR: un approccio basato sul rischio*, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 663.

La necessità di questo approccio deriva dal prendere atto che «*la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta dei dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.*

Sempre più spesso le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che ci riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali» (Cons. n. 6 GDPR). «*Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione affiancato ad efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche*» (Cons. n. 7 GDPR).

3. Il documento informatico, come contenitore di dati

L'elemento che caratterizza questa impostazione è il dato personale in tanto in quanto contenuto in un documento informatico[3], perché è quest'ultimo che ha la peculiare caratteristica di essere trattato con i

[3] Il d.lgs. 7 marzo 2005 n. 82 (Codice dell'Amministrazione Digitale) all'art. 1 lett. p) definisce il documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; in contrapposizione al documento analogico (lett. p-bis) definito come la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

Già nel 1972, RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, aveva "profeticamente" individuato questa caratteristica. Sul punto la letteratura è amplissima, v. per tutti: ALPA, *A proposito della ristampa anastatica di "Elaboratori elettronici e controllo sociale"*, in *Riv. crit. dir. priv.*, 2019, 137.

V. anche: PESCE, *Sul rapporto tra atto del privato inserito sulla piattaforma tecnologica "sicura ed irretrattabile" (blockchain) e atto pubblico. Riflessi sul procedimento e sul processo*, in *www.Judicium.it*, 7 settembre 2021.

sistemi informatici e dunque di essere messo in circolazione e condiviso in ambiti anche lontani dalla sfera personale del titolare del dato.

Questa radicale trasformazione dei dati è stata già da tempo oggetto di attenzione sia da parte del legislatore comunitario[4] che del legislatore nazionale in ambiti determinanti della vita sociale ed economica[5].

Le problematiche da ciò derivanti sono state evidenziate sotto moltissimi profili[6], ma la prospettiva assunta dal GDPR prende atto del fatto che la libera circolazione dei dati possa costituire un fattore di sviluppo economico.

Ciò che va dunque indagato è se il sistema normativo contenuto negli artt. 32, 33 e 34 del GDPR consente di realizzare un bilanciamento tra la necessità di tutela della libertà e dignità personale[7] e le esigenze di sviluppo dell'economia digitale fondata sullo scambio delle informazioni.

L'eccezionale attitudine delle reti informatiche a far circolare e condividere i documenti informatici, combinata con l'attitudine di questi ultimi di essere trattati per l'acquisizione delle più diverse informazioni che contengono, ha determinato dei profondissimi mutamenti praticamente in tutti i settori economici, come è stato correttamente rilevato da attenta dottrina (anche solo con riferimento alle email)[8] ed incide anche sulla tutela dei dati personali la cui protezione appare ancora più determinante[9].

---

[4] A partire dalla Convenzione del Consiglio d'Europa n. 108 del 28 gennaio 1981 c.d. Convenzione di Strasburgo sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (ratificata dall'Italia con L. 21 dicembre 1989 n. 98), e dalla Carta dei Diritti fondamentali dell'Unione Europea c.d. CEDU del 7 dicembre 2000.

[5] CONTALDO e GORGA, *Le regole tecniche del nuovo casellario giudiziale telematico*, in *Diritto dell'Internet*, n. 4/2008, 411; LISI e CONFANTE, *La conservazione digitale dei documenti contabili e fiscali alla luce della Circolare 3C/E dell'Agenzia delle Entrate*, in *Diritto dell'Internet*, 4/2007, 407; MACRÌ, *Gli strumenti per il dialogo dell'amministrazione digitale*, in *Azienditalia*, 5/2011, 856.

[6] Uno per tutti: MEZZANOTTE, *La memoria conservata in Internet ed il diritto all'oblio telematico: storia di uno scontro annunciato*, in *Diritto dell'Internet*, 4/2007, 398.

[7] LIBERATI BUCCIANTI, *Disposizioni Generali*, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 21.

[8] CERDONIO CHIAROMONTE, *Il valore dell'email nel quadro della disciplina dei documenti informatici*, in *Riv. dir. civ.*, 3/2021, 427.

[9] FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. It.*, luglio 2019, 1670.

4. Specificazione dell'*accountability* per la sicurezza dei dati

Dunque, l'obbligo di garantire la sicurezza nel trattamento dei dati è delineato dal GDPR in modo "elastico" quale declinazione concreta del principio di *accountability*, che può essere tradotto con responsabilità e insieme prova della responsabilità, con un particolare accento posto sulla dimostrazione di come viene esercitata la responsabilità e sulla sua verificabilità.

Com'è oramai noto, l'accountability poggia su due principi: l'adozione di misure tecniche ed organizzative adeguate a garantire il livello di sicurezza in relazione allo specifico rischio derivante dal quel trattamento dei dati e la possibilità di dimostrare in qualsiasi momento di avere adottato tali misure.

Il Parere n. 3/2010 del Gruppo di Lavoro articolo 29 ha messo in luce la circostanza che la flessibilità di tale principio possa non essere sufficiente a garantire la certezza del diritto[10] ed in effetti il rilevo non è di carattere secondario.

Tuttavia, la necessità di stabilire un criterio generale adottabile a tutte le circostanze ha portato il legislatore europeo ha recepire il principio dell'accountability, non senza introdurre l'indicazione di alcune misure minime (art. 32 lett da a a d), nonché alcune misure ulteriori come l'adesione a codici di condotta (art. 40) o a meccanismi di certificazione (art. 42).

L'importanza della "posta in gioco" e la delicatezza della materia relativa al trattamento dei dati personali hanno dunque portato a delineare un dovere di sicurezza che non si esaurisce nella predeterminazione di misure minime o di una determinata soglia di conformità e che, di contro, prevede una verifica sempre aggiornata dei profili di rischio.

In aggiunta a ciò, l'art. 25 del GDPR prescrive che il titolare del trattamento possa mettere in atto misure tecniche e organizzative adeguate già dal momento in cui deve determinare i mezzi del trattamento, sempre nell'ambito della dovuta contestualizzazione dell'attività posta o da porre in essere e cioè facendo in modo che gli strumenti tecnologici adoperati per il trattamento siano concepiti per pseudonomizzare e per raccogliere il numero minimo indispensabile di dati per la finalità indicata: si tratta del c.d. approccio *privacy by design*[11].

---

[10] Parere n. 3/2010 Gruppo di Lavoro Articolo 29 in www.garanteprivacy.it/documents/10160/10704, 14.

[11] CAVOUKIAN, *Privacy by Design, the 7 Foundational Principles*, in *www.privacysecurityacademy.com/wp-content/uploads/2020/08/PbD-Principles-and-Mapping.pdf*; MONTANARI, *Le misure tecniche ed organizzative come criterio concreto di comportamento*

Inoltre, l'art. 25 del GDPR prevede che il titolare del trattamento debba effettuare una valutazione d'impatto dei rischi previsti sulla protezione dei dati personali, quando un tipo di trattamento preveda l'uso di nuove tecnologie, sempre nell'ambito di una precisa valutazione del contesto in cui opera. La valutazione d'impatto (o DPIA) è svolta con la consultazione del responsabile della protezione dei dati, se nominato.

È stato osservato che la DPIA non è soggetta a pubblicazione o comunicazione, non essendo un documento pubblico[12].

Nondimeno appare evidente che tale attività costituisca un momento cruciale nella *accountability* di un determinato trattamento dei dati. La capacità del titolare del trattamento di valutare *ex ante* i rischi di quel trattamento, di mettere in atto le misure adeguate, informandone il DPO costituiscono elementi di valutazione del suo adempimento all'obbligo di garantire la sicurezza[13].

Completano il quadro delle misure di *accountability* l'adesione ai codici di condotta e la certificazione.

Senza eccedere i limiti di questi appunti, si può sinteticamente ricordare che i codici di condotta previsti dall'art. 40 del GPDR costituiscono un peculiare ed innovativo sistema autoregolamentare che, a differenza degli schemi autodisciplinari adottati nei diversi ambiti socio-economici frutto di autonomia negoziale, postula in vario modo un'ingerenza dei poteri pubblici[14], mentre la certificazione prevista dall'art. 42 rientra in quei modelli di comportamento volti a certificare la conformità di un servizio (o di un bene) a predeterminati parametri stabiliti[15].

Questo è ciò che si intende per "adeguatezza" ai sensi dell'art. 32, esprimendo quindi un principio che lungi dall'apparire generico o vago, si riempie della sostanza concreta delle azioni ed adempimenti che ciascun titolare del trattamento avrà valutato opportune in quel determinato momento

---

nella privacy by design, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 530;

[12] D'IPPOLITO, *La valutazione d'impatto introdotta dal GDPR: un approccio basato sul rischio*, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 671.

[13] Con particolare riferimento alle nuove tecnologie come l'intelligenza artificiale, il *machine learning*, l'*Internet of Things* e il *cloud computing* la DPIA diventa un momento cruciale nel bilanciamento fra protezione dei dati personali e iniziativa economica e incentivo all'innovazione e al progresso tecnologico: BATTELLI, *DPIA e le nuove tecnologie*, in *Comm. del cod. civ.*, vol. II, cit., 678.

[14] D'ORAZIO, *Codici di condotta*, in *Comm. del cod. civ.*, cit., 807.

[15] Mi sia consentito rinviare a BIANCA, *Art. 42 Lo scopo della norma*, in BARBA e PAGLIANTINI (a cura di) *Comm. del cod. civ.*, vol. II, Torino, 2019, 837.

per fronteggiare i rischi di *data breach* e svolgere le proprie attività in sicurezza[16].

5. Il *data breach* e le conseguenze risarcitorie

Nonostante le misure previste per garantire la sicurezza nel trattamento dei dati, gli episodi di indebita diffusione di dati e in senso più lato di *data breach* si verificano comunque.

Ciò significa che – a dispetto delle misure attuate in conformità al principio di *accountability* – la protezione dei dati non è stata garantita.

Di fronte a questa evidenza si rende necessario cominciare ad indagare le prospettive concrete di valutazione della responsabilità del titolare del trattamento e di quantificazione del pregiudizio arrecato ai titolari dei dati.

Il tema appare vieppiù complesso con riferimento agli episodi di *data breach* compiuti dai *cyber* criminali, i quali riescono ad entrare nei *data center* per prelevare i dati ivi contenti, oppure per bloccare l'accesso al *data center* da parte del titolare del trattamento per costringere quest'ultimo a pagare un riscatto per rientrare nella disponibilità dei dati.

In realtà, nessuno ci dice che l'*hacker* – una volta inserito il *ransomware* – non estragga anche una copia dei dati (o una parte di essi) in aggiunta alla richiesta di riscatto, per poi rivenderli.

Certo è che una volta violato il *data center* di un titolare del trattamento è molto difficile capire dove vadano a finire i dati abusivamente prelevati e chi tragga profitto da ciò.

In questo contesto è plausibile ritenere che sia difficile individuare il fatto-danno e dargli una quantificazione.

La giurisprudenza che fino ad ora ha avuto occasione di esaminare fattispecie di indebito trattamento dei dati (situazione per la verità in parte diversa dal data breach frutto di *cyber crime*) ha necessariamente dovuto applicare le norme della responsabilità aquiliana, con esiti per la verità non proprio soddisfacenti [17].

In un caso, addirittura, la diffusione illecita sul *web* del dato personale (una fotografia) è stata degradata da illecito ex art. 82 GDPR ad "inconveniente" e l'esistenza di un "serio pregiudizio" è stata esclusa in ragione della supposta

[16] GAMBINI, *Algoritmi e sicurezza*, in *Giur. It.*, 2019, 1726.

[17] Cass. Civ. Sez. I, ord. 10.06.2021 n. 16402; Cass. Civ., Sez. III, ord. 23/10/2020, n. 23390; Cass. Civ., Sez. VI-1, ord. 20/08/2020 n. 17383; Cass. Civ., Sez. I, ord., 19/02/2021 n. 4475; Trib. Torino 18/01/2020 in www.onelegale.it.

brevità della permanenza del dato in questione sul sito *web* del titolare del trattamento (una testata giornalistica)[18].

Il caso appare interessante sotto due profili: da un lato il mancato riconoscimento della violazione dell'art. 82 GDPR in favore della responsabilità aquiliana dell'art. 2043 c.c. con le arcinote conseguenze in ordine al regime di prova del danno e della colpa dell'autore dell'illecito trattamento del dato personale; dall'altro il mancato riconoscimento della serietà del pregiudizio.

Specialmente quest'ultimo aspetto merita di essere oggetto di riflessione, dal momento che non sembra sia stato adeguatamente preso in considerazione il fatto che la rimozione di un dato personale da una pagina *web* non assicuri affatto l'eliminazione totale del dato dalla rete [19] e quindi la rapidità della rimozione del dato personale dalla pagine *web* non diminuisce la gravità dell'illecito.

Ci si domanda se nei confronti di fattispecie del genere non sia più adeguata una risposta come quella prospettata da autorevole dottrina[20], la quale ha ipotizzato l'introduzione di un criterio risarcitorio non più basato sull'errore e sulla colpa, ma piuttosto sull'allocazione del rischio.

In altre parole, si ipotizza di prevedere dei meccanismi di allocazione del costo del danno cagionato su quei soggetti che astrattamente potrebbero essere responsabili mediante, ad esempio, la costituzione di un fondo al quale attingere, a prescindere dalle modalità dell'incidente o dell'errore.

Va precisato che questa dottrina fa riferimento alle ipotesi di responsabilità nel caso di applicazioni di intelligenza artificiale, ma forse anche per le fattispecie dannose relative agli episodi di *data breach* si potrebbe ipotizzare una soluzione del genere, se si pensa al fatto che entrambe i fenomeni (*A.I.* e *data breach*) partono dal presupposto comune di una realtà sociale ed economica sempre digitalmente interconnessa dove i dati e le informazioni sono destinate sin dall'origine ad una circolazione globale.

Potrebbe non essere azzardato ipotizzare che il Reg. UE 679/16, pur non essendo stato concepito per le applicazioni di intelligenza artificiale e per i *Big Data*, possa tuttavia contenere gli strumenti adeguati per un nuovo modello culturale e giuridico di riferimento che contemperi l'esigenza di tutelare la dignità della persona e non compromettere la creazione di un clima di fiducia che consenta lo sviluppo dell'economia digitale (Cons. n. 7).

---

[18] Trib. Torino, 18/01/2020, cit.

[19] C.G.U.E. sent. Causa C-507/17 del 24.09.2019

[20] FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it*., luglio 2019, 1675