LA RESPONSABILITA' CIVILE DA ILLECITO TRATTAMENTO DEI DATI PERSONALI

di GABRIELE BORGHI

Sommario: 1. La responsabilità civile cd. speciale nel prisma dell'art. 82 del GDPR – 2. Il nuovo principio di responsabilizzazione: la responsabilità civile in funzione preventiva – 3. L'analisi e la gestione del rischio nell'attività di trattamento dei dati personali.

1. La responsabilità civile cd. speciale nel prisma dell'art. 82 del GDPR

A seguito dell'abrogazione dell'art. 15 del D.Lgs. n. 196/2003, ad opera dell'art. 27 comma 1 lettera a) n. 2 del D.Lgs. n. 101/2018, l'art. 82[1] del Regolamento UE n. 2016/679 (GDPR) costituisce, allo stato attuale, l'unica norma di diritto sostanziale che riconosce, in modo specifico, il diritto al risarcimento del danno (patrimoniale e non patrimoniale[2]) conseguente ad un illecito trattamento dei dati personali.

[1] Si impone un'operazione ermeneutica estensiva dell'art. 82 del GDPR, posto che non può ritenersi che il diritto al risarcimento del danno alla privacy sussista unicamente nel caso in cui il danno sia causato da una violazione del GDPR; una siffatta interpretazione restrittiva si porrebbe, infatti, in contrasto sia con il Considerando n. 146 sia con il Considerando n. 80, giacché quest'ultimo spiega testualmente che con la locuzione "*trattamento non conforme al presente regolamento*" si intende anche "*il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento"*. A parere di chi scrive, anche la violazione di atti di cd. s*oft law*, adottati da parte del Garante della Privacy, legittima chiunque abbia subito un danno derivante da tale violazione a far valere il suo diritto in giudizio per fini risarcitori.

[2] La tematica della risarcibilità dei danni non patrimoniali (sovente connessi alla tutela dell'immagine, del decoro e della dignità dell'essere umano) risente dell'altalenante giurisprudenza

Dall'analisi della complessa formulazione della normativa in parola – composta da ben sei paragrafi – si evince che la stessa possieda le caratteristiche di una responsabilità civile cd. speciale, giacché il Legislatore comunitario ha ritenuto di andare ben oltre al generico impianto della responsabilità civile cd. comune (la quale, a parere della dottrina dominante, consiste nella responsabilità del *chiunque*, ossia di un soggetto non qualificato che pone in essere una condotta illecita contraria all'ordinamento giuridico), statuendo espressamente che le figure soggettive tipizzate (ossia, il Titolare ed il Responsabile del trattamento, nell'ambito delle rispettive competenze previste dal GDPR) siano gravate tanto da obblighi di condotta tipici, articolati e complessi quanto da disposizioni di principio – tra le quali primeggia quello di *accountability* – che investono, a prescindere dalla sussistenza o meno di un rapporto contrattuale con il soggetto interessato, tutta la loro attività.

Si registra, dunque, nell'impianto complessivo del nuovo regolamento comunitario un marcato cambio di visione rispetto alla previgente Direttiva CE n. 95/46: infatti, il Legislatore eurounitario ha spostato l'attenzione della prospettiva regolatoria dalla mera autodeterminazione mediante declinazione dei diritti e garanzie del soggetto interessato (da attuare in caso di violazione delle regole del trattamento) alla più moderna ed efficiente gestione e prevenzione del rischio del trattamento da parte del Titolare e/o del Responsabile, sul presupposto, peraltro, della natura imprenditoriale del trattamento di dati (altrui).

Altresì, si osserva, nello specifico, che la tutela procedimentale prevista dal GDPR – posta a presidio della liceità, correttezza e trasparenza del trattamento dei dati personali – non è diretta esclusivamente alla protezione dei

in materia la quale ha, talvolta, negato il risarcimento dei danni alla privacy sulla scorta della prevalenza del principio di tolleranza su quello di legalità, stante l'accertata tenuità della lesione subita dal soggetto danneggiato; in via generale, è, altresì, necessario ricordare che la giurisprudenza ha, da tempo, sposato il principio del cd. danno conseguenza, negando la sussistenza di un danno *in re ipsa* derivante dalla mera violazione della disciplina sul trattamento dei dati personali ed imponendo al danneggiato, onde vedersi accordato il risarcimento, la dimostrazione – anche mediante il mezzo presuntivo – di un effettivo pregiudizio prodottosi nella propria sfera giuridico-economica: cfr. *ex plurimis*: Corte di Cassazione Sez. I Ord. n. 207 del 8.1.2019.

diritti fondamentali e delle libertà individuali del soggetto interessato, ma anche a tutela di interessi collettivi di categoria tesi al buon funzionamento del mercato e dell'ordinamento giuridico in generale.

In tale ottica, risulta, quindi, coerente la scelta, operata dal Legislatore comunitario, di lasciare indeterminata la categoria dei soggetti tutelati, giacché, ai sensi dell'art. 82 del GDPR, "*chiunque*" subisce un danno può attivare il rimedio risarcitorio: nello specifico, il danneggiato, seppur indeterminato, può essere soltanto una persona fisica in ossequio al Considerando n. 14 del GDPR e, per altro verso, può essere, altresì, un soggetto differente rispetto all'interessato purché riesca a dimostrare di aver subito "*un pregiudizio di natura diversa dal trattamento di dati personali altrui*", avendo fatto legittimo affidamento sull'esattezza e completezza di tali dati.

Per tali ragioni, è opportuno inquadrare l'art. 82 GDPR all'interno dell'alveo della responsabilità extracontrattuale, atteso che è proprio il danno cagionato dal Titolare o dal Responsabile del trattamento a costituire un nesso di relazione con la sfera giuridica del soggetto interessato, potendo escludersi, siffatta responsabilità, soltanto mediante la prova (diabolica), posta in capo agli asseriti danneggianti, circa la non imputabilità dell'evento dannoso registratosi[3].

2. Il nuovo principio di responsabilizzazione: la responsabilità civile in funzione preventiva

L'appena descritto cambio di prospettiva deriva dal citato principio di *accountability*[4], il quale non solo caratterizza ed

[3] L'inversione dell'onere della prova che la norma europea dispone consente, per un verso, di aumentare la protezione del danneggiato, stante la difficoltà che questi potrebbe incontrare – in specie in riferimento alla realtà digitale in cui oggi si svolge la maggior parte dei trattamenti dei dati personali – nel dimostrare la colpa dell'autore del trattamento; per altro verso, permette di responsabilizzare il soggetto attivo del trattamento, il quale, per andare esente da responsabilità, non può limitarsi a fornire la prova negativa di non aver commesso alcuna violazione ma ha l'onere di dare la prova positiva di aver impiegato tutte le misure di prevenzione ragionevoli e comunque normalmente adeguate a scongiurare il danno, essendo, peraltro, tenuto a stare al passo con il progresso tecnologico e ad aggiornare le misure adottate al continuo evolvere delle tecniche di prevenzione del danno.

[4] Tale concetto è già presente dal 1980 nelle Linee Guida della OECD (*Organisation for Economic Cooperation and Development*), in base alle quali "*Un Titolare del trattamento dei dati dovrebbe essere responsabile per il rispetto delle misure che danno attuazione ai principi*" ("*A data controller should be accountable for complying with measures which give effect to the [material] principles stated above*"). Inoltre, all'interno del parere n. 3/2010 a firma del Gruppo di lavoro Art.

informa la nuova normativa europea sulla protezione dei dati ma manifesta, in particolar modo, un nuovo orientamento di politica del diritto, basato sulla gestione del rischio.

Infatti, il GDPR non prevede più soltanto prescrizioni dirette e precise alla cui mancata applicazione segue l'irrogazione di una sanzione (si pensi alle misure minime di sicurezza previste dal Legislatore italiano, contenute nell'Allegato b) del Codice della Privacy, oggi abrogato), bensì, all'opposto, si fonda su un obiettivo da realizzare secondo modalità (che saranno poi oggetto di successiva valutazione da parte dell'autorità di controllo e del giudice) che lo stesso Titolare e/o Responsabile del trattamento deve, di volta in volta, determinare in ragione della maggiore responsabilizzazione.

Si passa, dunque, da un approccio normativo che dettava indicazioni assai precise ad uno che impone a tali soggetti di modulare la concreta attuazione dei principi sanciti, in astratto, dalla normativa in materia.

A tal riguardo, si osserva, altresì, che l'*accountability* viene descritto come un meccanismo a due livelli, uno obbligatorio ed uno, invece, volontario: il primo livello sarebbe costituito da un obbligo di base vincolante per tutti i Titolari (e Responsabili) del trattamento, e comprenderebbe l'attuazione e la formalizzazione delle misure e/o procedure (es. adozione di un modello organizzativo) nonché la conservazione delle relative prove; viceversa, il secondo livello includerebbe sistemi di responsabilità di natura volontaria eccedenti le norme di legge cd. minime, in relazione ai principi fondamentali di protezione dei dati e/o in termine di modalità di attuazione o di garanzia dell'efficacia delle misure poste in essere.

Sulla scorta di ciò, si può affermare che tale principio configuri un modello di responsabilità volto alla prevenzione del danno, al punto che la responsabilità civile può essere definitiva soltanto una delle epifanie dell'*accountability*; in altri termini, la

29 per la protezione dei dati è stato affermato che tale termine può essere tradotto in differenti modi, fra i quali: responsabilità; affidabilità; assicurazione; obbligo di rendicontare; attuazione dei principi concernenti il trattamento dei dati personali. Infine, sull'*accountability* si segnala il ruolo trainante del progetto ''*Accountability- Based Privacy Governance*'' promosso da *The Centre for Information Policy Leadership* che ha coinvolto circa 60 partecipanti internazionali, fra i quali Garanti, industrie ed accademici.

responsabilizzazione *ex ante* si declina come responsabilità *ex post*[5].

3. L'analisi e la gestione del rischio nell'attività di trattamento dei dati personali

Tenuto a mente quanto poc'anzi affermato, è opportuno ora osservare che l'ambito nel quale il principio di *accountability* ha – senza dubbio – un'applicazione più evidente è quello della sicurezza dei dati personali; per raggiungere tale obiettivo, il GDPR impone al Titolare (e al Responsabile) del trattamento di adottare delle misure tecniche ed organizzative ritenute idonee a garantire un livello di sicurezza adeguato al rischio (di accessi, usi, modifiche, divulgazioni, perdite, distruzioni o danni accidentali, non autorizzati ovvero illegali).

Il processo teso alla scelta delle misure di sicurezza si articola nella fase di analisi e valutazione del rischio, ed in quella successiva rappresentata dalla gestione del rischio.

Per quanto concerne il primo aspetto, si deve ricordare, innanzitutto, che la valutazione del rischio[6], richiesta al Titolare ed al Responsabile del trattamento, è suscettibile di mutare in base al decorso del tempo, con la conseguenza che risulta di primaria importanza l'effettuazione della stessa in modo periodico e continuativo.

Tanto premesso, nell'ambito della sicurezza dei dati personali essa può articolarsi in quattro differenti fasi:

a. definizione dell'operazione di trattamento e del suo contesto: è necessario definire la natura del trattamento posto in essere, la tipologia dei dati personali trattati, le finalità di trattamento, gli strumenti utilizzati a tale scopo, i soggetti interessati ed, infine, gli eventuali destinatari dei dati trattati;

[5] In questo senso: E. Tosi, "*Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*", 2019, Giuffrè.

[6] Di solito, il calcolo del rischio si ricava dalla moltiplicazione tra la probabilità che una determinata minaccia presa in considerazione si verifichi ed il danno massimo ipotizzabile che può comportare quella medesima minaccia.

b. comprensione e valutazione dell'impatto: è opportuno valutare l'impatto che una possibile perdita di dati possa avere sui diritti e sulle libertà fondamentali delle persone fisiche;

c. definizione di possibili minacce e valutazione della loro probabilità[7]: risulta doveroso valutare a quali minacce (esterne o interne) è esposto il Titolare (e/o il Responsabile) del trattamento, sulla base del contesto in cui viene effettuato il trattamento preso in considerazione, oltre ché la probabilità che queste minacce si verifichino;

d. valutazione del rischio, da eseguirsi sulla base delle risultanze ottenute nelle fasi precedenti.

A seguito della valutazione del livello di rischio, il soggetto attivo del trattamento deve, quindi, procedere con la selezione delle misure di sicurezza appropriate ed adeguate per la protezione dei dati oggetto di trattamento, onde così diminuire – nella fase di gestione del rischio (*risk management*) – il valore della probabilità che un determinato evento lesivo si verifichi.

Nello specifico, le misure di sicurezza da scegliere devono, tuttavia, garantire, secondo i dettami del GDPR, che vengano trattati, per impostazione predefinita, soltanto i dati personali necessari per ogni specifica finalità di trattamento (*data protection by default*) e che, infine, la protezione dei dati sia garantita sin dalla fase di progettazione (*data protection by design*).

A tal uopo, gli strumenti utilizzabili sono da individuarsi nelle seguenti due macro categorie:

I. strumenti di natura tecnica: in via soltanto esemplificativa, se ne riportano alcuni: *a)* pseudonimizzazione dei dati personali: modalità di trattamento in cui i dati personali non possono essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive; *b)* cifratura dei dati personali: processo di codificazione e protezione delle informazioni, mediante l'utilizzo della crittografia e della criptoanalisi;

[7] Per fornire delle linee guida in tale fase, l'ENISA ha elaborato, all'interno del "*Manuale sulla sicurezza nel trattamento dei dati personali*" del Dicembre 2017, alcune domande che i soggetti attivi del trattamento possono farsi per comprendere il grado di esposizione dei dati personali trattati rispetto alle minacce informatiche e la probabilità che queste si verifichino.

c) back up periodici dei dati memorizzati; *d)* protezione della rete e dei propri sistemi attraverso dei controlli di accesso adeguati.

II. misure organizzative interne: ad esempio: *a)* trasmissione, in modo periodico, a tutto il proprio personale delle informazioni riguardanti le norme sulla sicurezza dei dati ed i connessi obblighi normativi; *b)* distribuzione chiara delle responsabilità e delineazione netta delle competenze in tema di trattamento dati; *c)* utilizzo dei dati personali soltanto in osservanza delle istruzioni impartite dalla persona competente ovvero in base alle norme vigenti in materia; *d)* protezione dell'accesso alle sedi, agli hardware e software, ivi inclusi i controlli relativi all'autorizzazione dell'accesso.

In conclusione, occorre, dunque, che il soggetto attivo del trattamento ponga in essere una complessa attività di valutazione (tecnica, giuridica ed organizzativa), un'analisi dei rischi e dei costi, una scelta sulle misure di sicurezza da adottare, l'istituzione di un presidio, l'emanazione di *policy* interne ed, infine, un attività di monitoraggio continuo e periodico.

Per di più, tutto ciò deve essere adeguatamente formalizzato ed attuato, onde così consentire al Titolare e/o al Responsabile del trattamento di assolvere all'onere della gravosa prova liberatoria impostagli per andare esente da eventuali ipotesi di responsabilità civile da trattamento illecito dei dati personali.