GIURIMETRICA

RIVISTA DI DIRITTO, BANCA E FINANZA

ANNO 7
NUMERO 1
GENNAIO/GIUGNO
2023

ISSN 2785-2547

alma iura
A VIA PER VIA

Mariafrancesca Cocuccio*

Violazione in materia di tutela di dati personali: profili di responsabilità civile

SOMMARIO

1. Premessa. - 2. La responsabilità civile per illecito trattamento dei dati personali alla luce del nuovo GDPR (*General Data Protection Regulation*). –3. *Segue*. Il principio dell'*accountability* (o principio di responsabilizzazione). - 4. Onere probatorio. – 5. Dati bancari e tutela risarcitoria. – 6. Dati particolari (ex dati sensibili) e ipotesi di trattamento lecito in ambito bancario.

1. Premessa. – Prima dell'entrata in vigore del Reg. (UE) 2016/ 679[1], nel nostro ordinamento il tema della responsabilità civile derivante da illecito trattamento dei dati personali[2] faceva riferimento all'art. 15 del d.lgs. 30 giugno 2003 n. 196 (*Codice in materia di protezione dei dati personali*), che statuiva: "*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11*".

La normativa originaria ancorava il trattamento dei dati personali a previsioni minime di sicurezza. L'art. 15 del Codice ricollegava, infatti, il trattamento illecito dei dati personali alla responsabilità civile prevista dall'art. 2050 c.c.

---

* Ricercatore di Diritto privato, Università di Messina.

1 Regolamento del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/ 46/ CE (regolamento generale sulla protezione dei dati). In dottrina cfr., AA.VV., Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018, (a cura di) R. Panetta, Milano, 2019; AA.VV., I dati personali nel diritto europeo, V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), Milano, 2019; Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel regolamento UE 2016/679, (a cura di) L. Califano e C. Colapietro, Napoli, 2018; AA.VV., Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali, a cura di G. Finocchiaro, Bologna, 2017; L. BOLOGNINI - E. PELINO - C. BISTOLFI, Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali, Milano, 2016; F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali, vol. I° (Dalla direttiva 95/46 al nuovo Regolamento europeo) e vol. II° (Il regolamento europeo 2016/679), Torino, 2016; M.G. STANZIONE, Il regolamento europeo sulla privacy: origini e ambito di applicazione, in Eur. dir. priv., 2016, 1249 ss.; A. SPINA, Alla ricerca di un modello di regolazione per l'economia dei dati. Commento al regolamento (Ue) 2016/679, in Riv. regolaz. merc., 2016, 143 ss.

2 Per dato personale si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale" (art. 4, GDPR).

per i casi di esercizio di attività pericolosa e sanciva, inoltre, la risarcibilità del danno non patrimoniale (art. 2059 c.c.)[3]. Ciò comportava che il titolare del trattamento era tenuto al risarcimento per i danni eventualmente prodotti, se non avesse provato di avere adottato tutte le misure idonee a evitarli.

La nuova disciplina sulla protezione dei dati, invece, individua come unico referente normativo della responsabilità civile in materia di trattamento illecito dei dati personali l'art. 82 del GDPR, che, al comma 1, stabilisce: "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*"[4].

Si è così introdotta una nuova normativa, differenziando la posizione del titolare da quella del responsabile del trattamento, prevedendo uno

---

3 Cass. Civ., 26 aprile 2021 n.11020, per la quale "risponde dei danni determinati dall'illecita divulgazione di dati personali, ai sensi dell'art. 15, comma 1, d. lgs. n. 196 del 2003 (applicabile ratione temporis) chiunque con la propria condotta li abbia provocati, indipendentemente dalla qualifica rivestita, di titolare o di responsabile del trattamento dati". In ordine al risarcimento dei danni, va preliminarmente osservato che si è già enunciato il principio di diritto secondo cui il danno non patrimoniale risarcibile, ai sensi del d.lgs. n. 196 del 2003, art. 15 (Codice della privacy), pur determinato da una lesione del diritto fondamentale alla protezione dei dati personali tutelato dagli artt. 2 e 21 Cost. e dall'art. 8 della CEDU, non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno", in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost., da cui deriva (come intrinseco precipitato) quello di tolleranza della lesione minima. Sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni poste dall'art. 11 del codice della privacy, ma solo quella che ne offenda in modo sensibile la sua portata effettiva, restando comunque il relativo accertamento di fatto rimesso al giudice di merito.
V. anche Cass. Civ., 20 agosto 2020 n. 17383; Cass. Civ., 17 settembre 2020 n. 19328, in Nuova giur. civ. comm., 1, 2021, 142 ss., con nota di C. SOLINAS, Danno non patrimoniale e violazione del diritto alla protezione dei dati personali, nella quale il Supremo Collegio, prendendo spunto da una fattispecie comunque soggetta, ratione temporis, al pregresso ordito normativo (art. 15 Codice privacy), ha avuto modo di affermare, sia pure in via incidentale e sfumata, come detto regime trova conferma pure nel nuovo GDPR (art. 82.3), giacché in esso, sulla base del principio di responsabilizzazione (accountability), viene posto a carico del soggetto titolare (eventualmente in solido con il responsabile) il rischio tipico della sua attività d'impresa, sulla scia di quanto previsto dall'art. 2050 c.c.
Una posizione di segno diverso, più prossima a quanto sostenuto nel testo sembra, invece, affiorare nel formante dottrinale, dove non mancano voci propense a sottolineare alcune peculiarità della nuova disciplina, irriducibili al modello regolativo ormai abrogato: cfr. C. SOLINAS, op. ult. cit., 148, la quale, all'esito di più articolate considerazioni, rileva come nell'attuale GDPR "per individuare i contorni della responsabilità e l'esatto contenuto della prova liberatoria non si possa più automaticamente far riferimento all'art. 2050 c.c., risultato decisivo per le soluzioni affermatesi nel precedente regime".

4 L'art. 82 diventa "norma di collegamento" con la suddetta disciplina codicistica, il che è una soluzione plausibile sul piano culturale, nel senso che la disposizione di provenienza europea si "alimenta" del formante legislativo del contesto in cui viene trasfusa. In altre parole, il danno da trattamento dei dati personali riceve tutela ai sensi dell'art. 82, applicato ed implementato dalla lex aquiliana della tradizione italiana: S. SICA, Art. 82. Diritto al risarcimento e responsabilità, in Codice della privacy e data protection, R. D'ORAZIO - G. FINOCCHARO- O POLLICINO – G. RESTA (a cura di), Milano, 2021, 892; E. LUCCHINI GUASTALLA, Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori, in Contr. impr., 2018, 108 ss.

speciale criterio di imputazione della responsabilità[5]. In particolare, sulla qualificazione giuridica della responsabilità civile per trattamento illecito di dati personali, se la dottrina dominante la inquadra in termini di responsabilità extracontrattuale[6], altro orientamento si è espresso in termini di responsabilità oggettiva (per rischio d'impresa) derivante dall'attività di trattamento dei dati personali in violazione delle regole di condotta conformative e protettive dell'interessato (danneggiato), soggetto debole del rapporto asimmetrico che il trattamento dei dati personali comporta. In base al principio del rischio d'impresa e al correlato parametro di efficienza, anche sotto il profilo dell'analisi economico-giuridica, (costi-benefici) "la responsabilità deve essere attribuita a chi ha il controllo delle condizioni generali del rischio ed è in grado di tradurre il rischio in costo inserendolo armonicamente nel gioco dei profitti e delle perdite, con lo strumento dell'assicurazione o dell'autotassazione"[7].

Altra dottrina, invece, individua nell'articolo 1218 c.c. la norma di riferimento di tale responsabilità: in virtù degli obblighi di condotta minuziosamente definiti in base al principio di *accountability* previsti in capo al titolare e, in certi frangenti, direttamente in capo al responsabile del trattamento, la relazione che si instaura tra questi e l'interessato assume la veste di un "complesso rapporto giuridico". Tali obblighi di condotta, pur essendo di natura procedimentale e non attribuendo all'interessato una specifica utilità, precedono l'eventuale produzione del danno e rientrano nella controversa categoria delle obbligazioni *ex lege*[8]. Ed ancora, la posizione che configura la responsabilità ex art. 82 come una responsabilità aggravata per colpa presunta, poiché tale qualificazione, che contempla il profilo soggettivo,

5 Si ritiene che il contratto tra titolare e responsabile sia un contratto atipico valido in quanto posto a tutela di interessi meritevoli di protezione e purché rispetti i requisiti di forma e di contenuto previsti dal Regolamento. Con riguardo la forma del contratto si possono formulare delle ipotesi utili a individuare lo schema negoziale più adatto a tal fine. Il contratto di esternalizzazione o di outsourcing è tra le ipotesi maggiormente condivise: si tratta di un contratto atipico con cui un soggetto (outsourcer) affida ad un terzo (outsourcee) la gestione di alcune funzioni o alcuni servizi della propria organizzazione. Attraverso tale contratto, dunque, il titolare del trattamento designa un soggetto terzo ed esterno alla propria struttura a cui delegare determinate attività di trattamento e il cui agire le circoscritto all'istruzione impartite dal titolare e precisate nel contratto di esternalizzazione. Anche il mandato sembra prestarsi a strumento di regolazione del rapporto così come anche il modello contrattuale dell'appalto di servizi: F. PIZZETTI, Art. 28. Responsabile del trattamento, in Codice della privacy e data protection, R. D'ORAZIO - G. FINOCCHARO- O POLLICINO – G. RESTA (a cura di), Milano, 2021, 471.

6 G. RESTA – A. SALERNO, La responsabilità civile per il trattamento dei dati personali, in La responsabilità d'impresa, a cura di Alpa e Conte, Milano, 2015, p. 653 ss.; E. LUCCHINI GUASTALLA, op. cit., 106 ss., GAMBINI, Principio di responsabilità e tutela aquiliana dei dati personali, Napoli, 2018.

7 E. TOSI, Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale, Milano, 2019, 125.

8 F. BILOTTA, La responsabilità civile nel trattamento dei dati personali, in Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy), PANNETTA (a cura di), Milano, 2019, 453.

risulta più coerente al principio di *accountability* e potrebbe rilevarsi, in un'ottica funzionale preventiva, più efficace nella valorizzazione del rimedio risarcitorio[9].

Si tratta di orientamenti che prospettano, in modo evidente, una modulazione diversa della tutela, in special modo sotto il profilo della (maggiore o minore) facilità di accesso al rimedio risarcitorio. Da questo angolo visuale, si comprende però come la scelta tra le diverse opzioni ermeneutiche discende, più che dai gusti o dalle sensibilità dell'interprete, da una valutazione ponderata e bilanciata dei valori perseguiti dalla normativa, nel caso di specie rappresentata dal testo del GDPR. Non va, comunque, sottaciuto che un'attenta considerazione del quadro normativo suggerisce approdi ricostruttivi in parte diversi da quelli appena delineati. Si è, infatti, rilevato come la responsabilità per l'illecito trattamento dei dati non derivi dalla lesione occasionale ed episodica di un interesse altrui, ma dalla violazione di un rapporto già esistente tra soggetti esattamente determinati (il titolare e l'interessato) e scandito, quanto alla sua dinamica evolutiva, da una disciplina dettagliata del suo contenuto, oltre che da una serie di obblighi di protezione ben precisi (di matrice legale e convenzionale) finalizzati a preservare l'integrità della privacy individuale.

2. La responsabilità civile per illecito trattamento dei dati personali alla luce del GDPR (*General Data Protection Regulation*). – Il Reg. (UE) 2016/679[10] pone un criterio di imputazione autonomo di responsabilità, facendo espressamente riferimento ai soggetti legittimati (passivi) a cui tale criterio si riferisce: titolare e responsabile del trattamento. Il primo è colui che ''singolarmente o insieme ad altri determina le finalità e i mezzi del trattamento'' (art. 4, n. 7 del Regolamento); il responsabile, invece, è colui che tratta i dati personali per conto del titolare del trattamento (art. 4, n. 8 del Regolamento).

---

9 M. GAMBINI, Responsabilità e risarcimento nel trattamento dei dati personali, in CUFFARO, D'ORAZIO, RICCIUTO (a cura di), I dati personali nel diritto europeo, Torino, 2019, 1082; G. NAVONE, Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali, in Nuova leggi civ. comm., 2022, 132.

10 Al fine di armonizzare la disciplina italiana con le disposizioni europee in materia di protezione dei dati personali previste dal Regolamento Privacy UE/679/2016 è stato approvato il d.lgs. 10 agosto 2018 n.101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) che è entrato in vigore il 19 settembre 2018 apportando notevoli modifiche al d.lgs. 196/2003 (Codice privacy). Per un primo commento: F. PIZZETTI, Protezione dei dati personali in Italia tra GDPR e codice novellato, Torino, 2021; L. BOLOGNINI - E. PELINO, Codice privacy: tutte le novità del d.lgs. 101/2018, Milano, 2019; S. SCAGLIARINI, Il «nuovo» codice in materia di protezione dei dati personali. La normativa italiana dopo il d.lgs. 101/2018, Torino, 2019.

La responsabilità del titolare e quella del responsabile discendono da fatti diversi. Il titolare del trattamento (o i contitolari solidalmente tra loro) fermo restando il regresso interno in ragione dell'effettivo contributo causale di ciascuno al fatto dannoso, risponde per il danno derivante da trattamento dei dati in violazione delle regole stabilite dal GDPR (art. 82.2, primo periodo)[11]. Il responsabile del trattamento (o i corresponsabili solidalmente tra loro) fermo restando il regresso interno in ragione dell'effettivo contributo causale di ciascuno al fatto dannoso, risponde, invece, se non ha adempiuto gli obblighi del GDPR specificamente diretti ai responsabili del trattamento (si segnala, in particolare, l'art. 28 GDPR) o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento (art. 82.2, secondo periodo) [12].

In sintesi: il titolare è responsabile per qualunque danno che derivi dal trattamento cui ha dato avvio, da solo o in solido con altri. Per quanto riguarda, invece, il responsabile del trattamento, l'obbligazione di risarcimento segue sostanzialmente uno schema di compliance e lo stesso risponde in maniera più limitata per i danni cagionati solo nel caso di violazione degli obblighi a suo carico tra cui, peraltro, rientra quello di seguire le istruzioni del titolare. Il Regolamento precisa che deve trattarsi di istruzioni ''legittime''; dal che discende che il responsabile non risponde per danni eventualmente causati dal suo rifiuto di adeguarsi a istruzioni illegittime. Sembra in ogni caso che il responsabile non abbia l'onere di valutare la legittimità delle istruzioni del titolare, a meno che queste interferiscano con gli obblighi che il Regolamento pone direttamente a suo carico (ad esempio, se il titolare indica al responsabile di non attuare determinate misure di sicurezza). Le modalità e le finalità del trattamento sono, infatti, determinate dal titolare e, anzi, una interferenza in proposito da parte del responsabile rischierebbe di mutarne la qualifica in titolare del trattamento[13].

---

11 A titolo esemplificativo, disattendendo i precetti di cui all'art. 24 GDPR che richiedono al titolare di mettere in atto misure tecniche e organizzative adeguate al fine di garantire che il trattamento dei dati sia conforme al GDPR: E. TOSI, La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR), in Studium iuris, 2020, 1034. ID., Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'articolo 82 del GDPR Ue, in Danno e resp., 2020, 433; Illecito trattamento dei dati personali responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente sanzionatoria e rinascita del danno morale soggettivo, in Contratto impr., 2020, 1115.

12 R. CATERINA – S. THOBANI, Il diritto al risarcimento dei danni, in Giur. it., 2019, 2806; C. CAMARDI, Note critiche in tema di danno da illecito trattamento dei dati personali, in Ius civile, 2020, 786.

13 Ai fini della ripartizione interna della responsabilità tra titolare e responsabile si ha riguardo alla misura in cui il danno è stato causato dalle rispettive condotte: così, si accerta se il mancato rispetto da parte del responsabile degli obblighi posti a suo carico o delle legittime istruzioni del titolare sia dovuto anche a una condotta del titolare, il quale, ad esempio, potrebbe non aver fornito al responsabile adeguate indicazioni per consentirgli l'espletamento dei compiti affidatigli. Se, invece, il titolare ha posto il responsabile nella posizione di rispettare tutti gli obblighi a suo carico e quest'ultimo non lo ha fatto, il titolare potrà in

Sul titolare grava un'obbligazione risarcitoria "generale", mentre il responsabile se ne fa carico se non svolge esattamente i compiti che gli derivano dal Regolamento o se, di fronte ad indicazioni contro legem del titolare, non si astiene dal darvi attuazione. Tali profili concernono la sfera del rapporto (interno) di responsabilità tra i soggetti coinvolti, mentre su entrambi "pesa" quanto al rapporto con il danneggiato, la scura del comma 3, art. 82 GDPR[14].

È evidente che la responsabilità del titolare è più ampia rispetto a quella del responsabile: è il titolare a decidere di attuare il trattamento, determinandone finalità e modalità[15]. Il considerando n. 74 del Regolamento, infatti, afferma la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto[16]. Il titolare del trattamento è tenuto, sia a

linea di massima rivalersi per l'intero sul responsabile. Ci si può, tuttavia, chiedere se possa in alcuni casi residuare una responsabilità del titolare. L'ipotesi non pare del tutto da escludersi: si pensi, ad esempio, ad un titolare adeguatamente esperto che si avvale di un responsabile palesemente inesperto e inadeguato: R. CATERINA – S. THOBANI, op. cit., 2806. V. anche M. GIRAUDO, Responsabilità e danno nel caso di illecito trattamento dei dati personali, in Nuova giur. civ. comm., 2021, 1072.

14 S. SICA, op. cit., 890.

15 Da ultimo si v. le Conclusioni presentate il 27 aprile 2023 nella causa C340/21(VB vs Natsionalna agentsia za prihodite), dall'Avvocato generale della Corte UE (Giovanni Pitruzzella) che ha fornito indicazioni in materia di responsabilità del titolare del trattamento in caso di violazione dei dati personali per accesso illecito da parte di terzi. In particolare, l'Avvocato generale ha concluso nel senso che il titolare del trattamento dei dati personali è considerato responsabile per colpa presunta nel caso in cui terzi accedano illegalmente a tali dati, e ciò può comportare un risarcimento per danno morale. Tuttavia, il titolare del trattamento può essere esonerato da tale responsabilità dimostrando di non essere in alcun modo coinvolto nell'evento dannoso. Nel caso di specie la Corte UE è stata chiamata a definire, in base al regolamento generale sulla protezione dei dati, le condizioni per il risarcimento del danno morale subito da un soggetto i cui dati personali sono stati pubblicati illecitamente su internet da un'agenzia pubblica a seguito di un attacco hacker. Nelle sue conclusioni, si è evidenziato come il titolare del trattamento deve adottare misure tecniche e organizzative adeguate a garantire il rispetto del regolamento. L'adeguatezza di tali misure dipende dalla valutazione caso per caso. La violazione dei dati personali non implica necessariamente che le misure tecniche e organizzative adottate dal responsabile del trattamento non siano adeguate a garantire la protezione dei dati. Il giudice nazionale deve, invece, valutare in concreto l'adeguatezza delle misure di protezione dei dati, analizzando il contenuto delle stesse, il loro modo di applicazione e gli effetti pratici, al fine di garantire la protezione dei dati personali dei soggetti interessati. Per essere esonerato da responsabilità, il titolare del trattamento deve, quindi, dimostrare da un lato, l'adeguatezza delle misure tecniche e organizzative adottate, dall'altro, che l'evento dannoso non gli è in alcun modo imputabile. Se vi fosse il timore di un uso improprio dei dati personali ciò potrebbe costituire un danno morale che giustifica un risarcimento solo se si tratta di un danno emotivo reale e certo e non di un semplice disagio o fastidio.

16 L'articolo 82 del Regolamento europeo sancisce al primo paragrafo che chiunque subisca un danno "materiale o immateriale" (ossia, patrimoniale o non patrimoniale), causato da una violazione del GDPR, ha diritto ad ottenere il risarcimento del danno dal titolare o dal responsabile del trattamento dei dati personali. Viene così riconosciuta espressamente l'ammissibilità anche del danno non patrimoniale e vengono identificati gli elementi necessari per la nascita dell'obbligazione risarcitoria: la condotta attiva o quella omissiva contraria al regolamento; il danno; il rapporto causa-effetto tra questi. Il legislatore pone al centro della fattispecie il soggetto debole del rapporto, costruendo la disposizione attorno al danneggiato ed al suo diritto al risarcimento: M. COCUCCIO, Dimensione "patrimoniale" del dato personale e tutele

mettere in atto quelle misure tecniche e organizzative adeguate a garantire che il trattamento venga effettuato conformemente al presente regolamento, sia a riesaminare e aggiornare tali misure (art. 24 GDPR)[17]. L'art. 32, infatti, pone in capo al titolare e al responsabile l'obbligo di adottare ''misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio", tenuto conto ''dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche''. L'adozione delle misure di sicurezza è, quindi, considerata attività successiva ad una preliminare valutazione del trattamento, a partire dallo scopo perseguito, dalle categorie di dati trattati, dal probabile rischio a cui i dati potrebbero essere esposti, dai danni potenziali, dai costi e dallo stato dell'arte[18].

Dalla normativa europea emerge chiaramente la volontà del legislatore di instaurare un apparato di tutela in relazione ai trattamenti effettuati con strumenti elettronici, individuando gli oneri che il titolare del trattamento deve attuare per assicurare il necessario standard di sicurezza previsto.

Rispetto alla disciplina del 2003, si abbandona l'intento di ancorare i titolari

risarcitorie, in Dir. fam. pers., 2022, 230.

17 Sul punto si fa riferimento all'accountability (principio di responsabilizzazione). La disposizione ha lo scopo di promuovere l'adozione di misure concrete e pratiche, in quanto trasforma i principi generali della protezione dei dati in politiche e procedure concrete definite al livello del titolare del trattamento, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento deve anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Quindi previsione della responsabilità e prova delle misure adottate per fare fronte alla responsabilità. Secondo il Gruppo di lavoro Articolo 29 per la protezione dei dati, due sono gli elementi principali dell'accountability: ''(i) la necessità che il responsabile (N.d.A.: titolare) del trattamento adotti misure appropriate ed efficaci per attuare i principi di protezione dei dati; (ii) la necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto, il responsabile (N.d.A.: titolare) del trattamento deve fornire la prova di quanto esposto al punto (i)'': G. FINOCCHIARO, Il principio di accountibility, in Giur.it., 2019, 2778.

18 Nel definire le misure di sicurezza da adottare, il paragrafo 1 dell'articolo 32 prevede alla lettera b) "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento", alla lettera c) "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico" ed infine alla lettera d) il ricorso ad una procedura che ha l'obiettivo di "testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento". Il secondo paragrafo dell'articolo richiede, inoltre, che si valuti "l'adeguato livello di sicurezza" e che si tenga conto dei rischi presentati dal trattamento che derivano "dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati". Pertanto, la norma individua una serie di misure tecniche e di condotte che misurano il grado di diligenza che il responsabile del trattamento dei dati personali ha l'obbligo di adottare, dal punto di vista tecnico e organizzativo allo stesso tempo, essa pone in evidenza i rischi che potrebbero emergere dalla distruzione, dalla perdita o dalla modifica dei dati, e fa emergere la tipologia dei danni che potrebbero derivare dalla violazione dei necessari obblighi di protezione. In dottrina E. AINA, Brevi annotazioni sulla responsabilità da illecito trattamento dei dati personali, in Giur. it., 2013, 542.

del trattamento a previsioni minime di sicurezza preferendo, invece, la loro responsabilizzazione ed affidando ad essi l'incarico di comprendere l'importanza dei dati in proprio possesso; di decidere autonomamente le misure tecniche ed organizzative che si ritengono necessarie per assicurare la effettiva tutela dei dati personali, in considerazione della realtà produttiva in cui si opera; di dimostrare di aver adottato i necessari adempimenti con l'osservanza delle adeguate misure, per soddisfare gli standard di tutela richiesti.

3. *Segue*. Il principio dell'*accountability* (o principio di responsabilizzazione). - La normativa introdotta dal Regolamento europeo si concentra sul principio dell'accountability, che si sostanzia nell'obbligo posto in capo al titolare del trattamento dei dati personali di valutare le informazioni in loro possesso ed il loro conseguente valore, al fine di approntare le misure tecniche ed organizzative adeguate a mettere al sicuro tali dati. Ciò impone una gestione responsabile che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale. L'adozione di questo principio apre una nuova stagione nella protezione dei dati personali e manifesta un nuovo orientamento di politica del diritto.

In base alle regole di *accountability*, che segnano il passaggio dal previgente modello normativo ispirato alla prevalente, per non dire esclusiva, rilevanza della responsabilità *ex post* a un modello normativo evoluto e complesso centrato sulla valorizzazione, innanzitutto, ma non solo, della responsabilizzazione, consapevole e documentata, *ex ante*, i principi posti dalla nuova disciplina cessano di essere meri obblighi formali ed astratti per divenire obblighi adattabili e flessibili in relazione alle effettive esigenze applicative, emerse, caso per caso, in concreto, all'esito della doverosa analisi preliminare e autodiagnosi, specifica (*rectius* personalizzata) per ogni singolo titolare[19].

Il principio di *accountability* non comporta, però, soltanto la responsabilità di scegliere in quale modo dare attuazione alle prescrizioni del Regolamento, in quanto implica, altresì, l'onere di provare in quale modo il titolare ha effettivamente dato attuazione alle previsioni normative. Il Regolamento stesso suggerisce alcuni strumenti, fra i quali, ad esempio, le certificazioni e, agli artt. 42 e 43 precisa che esse, se ottenute, contribuiscono a dimostrare

19 E. TOSI, Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo, in Contratto e impresa, 2020, 1128.

la conformità al Regolamento dei trattamenti effettuati dai titolari del trattamento, ivi inclusa l'adeguatezza delle misure tecniche ed organizzative di sicurezza adottate. Tuttavia, il Regolamento aggiunge anche che questi strumenti, pur non riducendo la responsabilità dei titolari stessi nel caso in cui venga rilevata una loro inosservanza delle disposizioni del Regolamento, lasciano impregiudicati i compiti e i poteri delle autorità di controllo competenti.

Il processo decisionale complessivo che deve effettuare il titolare del trattamento e che muove dalla valutazione dell'esistente, dall'esame della natura dei dati e delle tipologie di trattamento, dalla ponderazione dei rischi e delle misure di sicurezza da adottare deve, quindi, essere documentato per potersi dimostrare l'attività effettuata[20].

Si parla generalmente di *accountability* come di un principio che risponde all'esigenza di fornire un parametro unico per tutte le situazioni di trattamento di dati personali ma, al tempo stesso, modulabile a seconda delle caratteristiche, dei compiti e delle finalità che ciascun titolare del trattamento persegue e dei trattamenti che attua tenendo conto anche della relativa base di legittimazione. Ed ancora di *accountability* può parlarsi in presenza di approcci variamente tendenti ad affidabilità, conformità, responsabilità, proattività nella gestione del trattamento dei dati personali. La responsabilizzazione del titolare del trattamento incarna, infatti, un'attività preventiva di valutazione e gestione del rischio che risulta idoneo, non solo in abstracto, a garantire nell'attività di trattamento dei dati personali, il rispetto dei principi di liceità, correttezza trasparenza, limitazione di finalità del trattamento, e di minimizzazione, esattezza, limitazione conservativa, integrità e riservatezza dei dati.

L'*accountability* è descritto come un meccanismo a due livelli, uno obbligatorio ed uno, invece, volontario: il primo sarebbe costituito da un obbligo di base vincolante per tutti i titolari (e responsabili) del trattamento, e comporta 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 include 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

20 G. FINOCCHIARO, op. cit., 2782: qualora il titolare adotti un modello organizzativo specifico, dovrà provvedere a formalizzarlo, eventualmente assumendo le deliberazioni necessarie. Nel caso in cui il rischio assunto vada monitorato, occorrerà anche predisporre un presidio organizzativo e di vigilanza.

o di garanzia dell'efficacia delle misure attuate[21]. La concretizzazione del principio di *accountability* impone, pertanto, al titolare di disporre le misure tecniche e organizzative adeguate a garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

L'introduzione del principio di *accountability* determina l'onere di adottare un nuovo approccio preventivo e responsabile nella gestione della protezione dei dati da parte delle singole organizzazioni aziendali, segnando l'emersione di complessi doveri di gestione e prevenzione differenziati in base al rischio specifico correlato al peculiare trattamento dei dati personali posto in essere[22].

Si è passati, in sostanza, dal principio di autodeterminazione mediante declinazione di diritti e garanzie dell'interessato, da attuare in caso di violazione delle regole del trattamento (direttiva 95/46), alla moderna concezione della gestione e prevenzione del rischio del trattamento che presuppone una natura del trattamento dati personali di tipo imprenditoriale (GDPR): in ciò, fondamentalmente, la novità del principio di responsabilizzazione *ex ante* rispetto al concetto di responsabilità *ex post*.

A questo principio si associa quello di proporzionalità: il trattamento dei dati deve essere proporzionato rispetto allo scopo legittimo perseguito e riflettere in tutte le fasi un giusto equilibrio tra tutti gli interessi coinvolti e i diritti e le libertà in gioco. Il trattamento dei dati personali deve essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va, infatti, contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a

---

21 In questo senso E. TOSI, Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale, cit., 139: 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 responsabilizzazione ex ante si declina come responsabilità ex post.

22 Il titolare del trattamento può valutare le scelte più consone al trattamento che concretamente effettua, considerando le circostanze del caso concreto che certamente non possono esser considerate dal legislatore ex ante, ma tali scelte sono sempre sottoposte ex post al controllo del giudice o del Garante. Dunque, mentre le prescrizioni normative delineano soluzioni per tutti i titolari non sempre adatte alla questione da affrontare, ma rassicuranti quanto all'avvenuto rispetto della norma, al contrario il principio dell'accountability crea libertà, ma insieme responsabilità: G. FINOCCHIARO, Il principio di accountability, in Giur.it., 2019, 2782.

un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Affinché una misura rispetti il principio di proporzionalità, i vantaggi derivanti dalla misura non dovrebbero essere compensati dagli svantaggi che la stessa comporta rispetto all'esercizio dei diritti fondamentali. Per adottare le misure di sicurezza adeguate in base al tipo di trattamento svolto, il titolare del trattamento deve effettuare un'analisi del rischio, vale a dire valutare tutti i possibili rischi che possono verificarsi in ordine ai dati trattati (art. 24 GDPR).

4. Onere probatorio. - La responsabilità in capo al titolare non si esaurisce con la valutazione e l'adozione delle misure di sicurezza (tecniche ed organizzative). Il titolare deve, infatti, compiere un'attività di continuo monitoraggio, per verificare che esse siano proporzionate e adeguate ai rischi, anch'essi in continuo mutamento[23]. Ciò significa che una volta effettuate le opportune valutazioni e adottate le conseguenti misure il titolare del trattamento dovrà continuare a mostrare una condotta attiva volta a testare, verificare e valutare regolarmente l'efficacia delle misure implementate.

Occorre, quindi, una complessa attività di valutazione (tecnica, giuridica e 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 e un'attività di monitoraggio continuo[24]. Pertanto, ai fini della ripartizione interna della responsabilità tra titolare e responsabile si avrà riguardo alla misura in cui il danno è stato causato dalle rispettive condotte: così, si dovrà accertare se il mancato rispetto da parte del responsabile degli obblighi posti a suo carico o delle legittime istruzioni del titolare sia dovuto anche a una condotta del titolare, il quale, ad esempio, potrebbe non aver fornito al responsabile adeguate indicazioni per consentirgli l'espletamento dei compiti affidatigli. Se, invece, il titolare ha posto il responsabile nella posizione di rispettare tutti gli obblighi a suo carico e quest'ultimo non lo ha fatto, il titolare potrà in linea di massima rivalersi per l'intero sul responsabile.

---

23 Non vale in ogni caso a escludere la responsabilità del titolare la prova che il danno è stato cagionato dal responsabile. Sembra al contrario che il responsabile possa liberarsi se riesce a dimostrare una causa del danno diversa dalla violazione dei propri obblighi. Così, se il responsabile prova che il danno è stato cagionato da uno specifico fatto del titolare, indipendente dall'attività di cui è stato incaricato, questo basterà a escluderne la responsabilità (e non dovrà a questo punto dimostrare di aver adempiuto i propri obblighi): R. CATERINA – S. THOBANI, Il diritto al risarcimento dei danni, cit., 2808.

24 Tutto ciò deve essere anche adeguatamente formalizzato e il titolare non deve attuare soltanto la normativa vigente, ma essere anche in grado di dimostrarlo: G. FINOCCHIARO, Il principio di accountibility, cit., 2781.

Sia il titolare che il responsabile del trattamento possono, però, andare esenti da responsabilità se dimostrano che l'evento dannoso non è loro "in alcun modo imputabile" (art. 82)[25]. È, infatti, sufficiente che il soggetto interessato dimostri la sussistenza di un trattamento, di un danno e del nesso causale tra il primo e il secondo[26]. A questo si aggiunga il fatto che deve provare che il danno deriva dal trattamento e che quel trattamento è riferibile al titolare o responsabile asseritamente danneggiante. Essi potranno liberarsi da responsabilità dimostrando che non vi è stata alcuna violazione, cioè, che il trattamento non si è posto al di fuori del perimetro di liceità delineato dal Regolamento (ad esempio: dimostrando il consenso al trattamento), che non erano disponibili misure tecniche atte a mitigare il rischio (purché il rischio di verificazione dei danni e l'entità degli stessi fossero sufficientemente bassi, dovendosi altrimenti astenere dal trattamento) o che i costi delle misure di prevenzione erano eccessivi rispetto a una bassa probabilità e/o gravità del rischio[27].

Il soggetto che effettua il trattamento per sottrarsi all'obbligo di risarcimento ha l'onere di provare di avere adottato tutte le misure idonee ad evitare il danno, secondo il principio dell'inversione dell'onere della prova, non essendo sufficiente dimostrare di non avere violato norme di legge o di prudenza. La ragione dell'inversione dell'onere della prova risiede nel fatto

---

25 Il Regolamento riprende e arricchisce quanto già previsto dal legislatore europeo con la previgente dir. n. 45/96/CE, rispetto a cui le maggiori novità consistono nell'aver specificato le rispettive responsabilità dei soggetti coinvolti nel trattamento e le tipologie di danni risarcibili. La direttiva, infatti, poneva l'obbligo per gli Stati membri di disporre che chiunque subisse un danno per effetto del trattamento illecito avesse il diritto di ottenere il risarcimento del pregiudizio dal responsabile del trattamento (che corrisponde all'attuale titolare), il quale poteva andare esente da responsabilità se dimostrava che l'evento dannoso non gli era imputabile (art. 23). Il legislatore italiano, invece, aveva scelto di non delimitare la legittimazione passiva, prevedendo che chiunque cagionasse un danno, anche non patrimoniale, per effetto del trattamento fosse tenuto al risarcimento (art. 15, d.lgs. n. 196/2003), e aveva disposto l'applicabilità del regime di responsabilità di cui all'art. 2050 c.c.: R. CATERINA – S. THOBANI, op. cit., 2805.
In giurisprudenza v. da ultima Cass. 12 maggio 2023 n. 13073, per la quale "in base alla disciplina generale del Regolamento (UE) 2016.679, cd. GDPR, il titolare del trattamento dei dati personali è sempre tenuto a risarcire il danno cagionato a una persona da un trattamento non conforme al regolamento stesso e può essere esonerato dalla responsabilità non semplicemente se si è attivato (come suo dovere) per rimuovere il dato illecitamente esposto, ma solo se dimostra che l'evento dannoso non gli è in alcun modo imputabile. L'esclusione del principio del danno in re ipsa presuppone, in questi casi, la prova della serietà della lesione conseguente al trattamento; ciò vuol dire che può non determinare il danno la mera violazione delle prescrizioni formali in tema di trattamento del dato, mentre induce sempre al risarcimento quella violazione che concretamente offenda la portata effettiva del diritto alla riservatezza".

26 L'interessato può fruire indirettamente di uno strumento di controllo dell'operato del titolare del trattamento, da azionare attraverso il ricorso all'autorità di controllo o, nei casi e secondo le modalità previste dal Regolamento, all'autorità giudiziaria, i quali potranno chiedere al titolare del trattamento di dimostrare che il trattamento è effettuato conformemente al regolamento: F. PIZZETTI, Art. 24. Responsabilità del titolare del trattamento, cit., 407.

27 M. RATTI, La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento, in G. FINOCCHIARO (a cura di), Il Nuovo Regolamento europeo sulla protezione dei dati personali, Bologna, 2017, 616, per il quale "si tratta di una responsabilità per colpa, in cui la colpa è presunta e qualificata".

che il trattamento dei dati è attività considerata pericolosa. Infatti, essa è consentita dall'ordinamento giuridico perché utile, con conseguente compensazione del rischio di violazione dei dati personali tramite l'obbligo a carico delle organizzazioni di garantirne la sicurezza dei trattamenti.

In altri termini, seguendo la logica dell'inversione dell'onere della prova, i soggetti coinvolti, per poter essere esonerati da responsabilità, dovranno provare che l'evento dannoso non è loro ascrivibile in quanto dipendente da una fonte estranea alla loro sfera di competenza o di controllo, oppure che sono state da loro predisposte ed attuate, in seguito alla valutazione dei rischi (art. 35 GDPR), tutte le prevedibili misure adeguate (art. 32 GDPR) al fine di evitare che si verificasse il danno. Diversamente, nel chiedere il risarcimento del danno[28], l'interessato dovrà provare l'esistenza del danno e la sua quantificazione, la sussistenza di una condotta in violazione della normativa a tutela dei dati personali e la relazione causale tra i primi due elementi.

5. Dati bancari e tutela risarcitoria. – In ambito bancario la tutela posta a carico dell'istituto di credito assume maggiore importanza se si considera che, oltre alle disposizioni in materia di dati sensibili, la banca è tenuta ad un generale obbligo di segretezza circa i dati patrimoniali e personali acquisiti per tramite i rapporti (bancari) con il cliente, ma più in generale di tutte quelle persone che entrano in contatto con il mondo bancario e i cui dati personali vengono, a vario titolo (e finalità) trattati[29].

La Banca deve attuare una serie di accorgimenti e di procedure semplici, snelle, chiare e trasparenti che consentono all'interessato, in qualsiasi momento, di controllare il trattamento dei propri dati e la corrispondenza di tale trattamento alle finalità e ai mezzi utilizzati. Deve, quindi, fornire al

---

28 L'impianto risarcitorio riconosce il diritto e la possibilità, a chi subisca un danno (non patrimoniale) dall'illecito trattamento di dati personali, di ottenere una tutela risarcitoria provando la gravità della lesione del diritto e la serietà del danno subito, ciò nel rispetto delle previsioni di cui all'art. 79 e 82 GDPR. In estrema sintesi, si può affermare che perché a seguito di illecito trattamento di dati personali vengano ad esistere i presupposti per il risarcimento del danno non patrimoniale, è necessario che: sia stato posto in essere un trattamento non conforme al GDPR o non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del GDPR e alle disposizioni del diritto degli Stati membri; il trattamento illecito dei dati abbia determinato la lesione di un diritto fondamentale dell'interessato; si sia verificato un danno conseguenza diretta della violazione stessa in materia di dati personali; il danno sia di non scarsa rilevanza o importanza.

29 La Banca può trattare i dati personali sia singolarmente che in maniera aggregata, utilizzando cioè un insieme di dati molto spesso presenti all'interno di data base sia digitali che analogici. L'Istituto di credito può trattare i dati personali con o senza l'ausilio di processi automatizzati; ciò significa che siamo di fronte a trattamento sia quando l'operatore bancario agisce utilizzando la tecnologia e gli strumenti informatici di cui può disporre, sia quando il medesimo operatore raccoglie i dati, li organizza, li registra li conserva, li consulta o li estrae da un fascicolo cartaceo piuttosto che da un archivio analogico.

soggetto interessato tutta una serie di informazioni che consentano il libero e consapevole esercizio del controllo dei propri dati personali; ciò attraverso una adeguata informativa.

L'istituto bancario che, violando i principi di liceità e correttezza, diffonde informazioni relative ad esempio alla posizione patrimoniale di un proprio correntista, risulta sanzionabile sia sul piano giuridico che deontologico. Ciò in quanto la condotta lede non solo il diritto alla riservatezza (art. 2 Cost.), ma anche quello all'inviolabilità e alla segretezza della corrispondenza e delle comunicazioni (art. 15 Cost.), trattandosi di informazioni strettamente personali per la natura ed il contenuto delle quali si dovrebbe garantire il massimo riserbo[30].

In caso, quindi, di illecito trattamento dei dati personali (e patrimoniali) da parte della banca (fattispecie che si verifica, ad esempio, mediante la divulgazione degli estratti conto del correntista o dei contratti di finanziamento che la banca ha realizzato con lo stesso) il cliente può ottenere il risarcimento del danno ai sensi dell'art 2050 c.c.

Una recente pronuncia della Corte di Cassazione ha statuito, in materia di protezione dei dati personali, l'illegittimità della condotta di una compagnia assicuratrice che aveva trasmesso al proprio assicurato, senza alcuna valida ragione e motivazione, anche le coordinate bancarie del soggetto risarcito[31]. A quest'ultimo, da tale illegittima diffusione ne sarebbe derivato "fastidio, preoccupazione, disagio", in quanto l'assicurato, in un secondo momento, le aveva esibite nel corso di un'assemblea condominiale di cui era parte lo stesso soggetto risarcito.

Orbene, nell'accogliere il ricorso, la Suprema Corte ha asserito che le coordinate

---

30 La banca deve adottare misure di sicurezza che garantiscono l'accesso ai dati personali solo a soggetti autorizzati, la completezza e l'accuratezza dei dati personali trattati per la specifica finalità e l'accessibilità, nonché l'utilizzabilità dei dati personali fornendo prova di essere in grado di recuperare e ripristinate in tempi rapidi i dati in caso di perdita, modifica o distruzione limitando al massimo i danni alle persone. Per quanto riguarda la sicurezza informatica è necessario valutare la sicurezza della rete e dei sistemi di informazione (c.d. sistemi di autenticazione), la sicurezza dei dati conservati nel sistema (c.d. controlli di accesso, la sicurezza online [sito web e/o applicazioni online]), nonché la sicurezza dei dispositivi, in particolare quelli personali se usati per motivi aziendali.

31 Cass. Civ., 19 febbraio 2021 n.4475, in Danno e resp., 2021, 486, con nota di C. NAPOLITANO, L'indebita divulgazione di codici Iban determina la violazione del diritto alla riservatezza. (Nella specie, la S.C. ha cassato la pronuncia di merito che aveva rigettato la domanda di risarcimento per l'illecita diffusione dei propri dati bancari, proposta dai danneggiati nei confronti della compagnia assicuratrice che li aveva risarciti in occasione di un sinistro, per avere indicato i dati stesso in calce all'atto di liquidazione trasmesso al proprio assicurato, il quale li aveva poi diffusi nel corso di una assemblea condominiale).

bancarie (iban) sono da qualificarsi come un dato personale ex art. 4, lett. b) del d.lgs. n. 196 del 2003 (nel testo, applicabile *ratione temporis*, anteriore alle modifiche apportate dal d. l. n. 201 del 2011, convertito, con modificazioni, dalla l. n. 214 del 2011) rientrando in tale nozione "qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale"[32]. L'iban deve essere trattato in modo lecito e secondo correttezza; inoltre, potrà essere raccolto, conservato e utilizzato solo per scopi determinati, espliciti e legittimi e non eccedenti rispetto alle finalità per le quali è raccolto; da ultimo, per un periodo di tempo non superiore rispetto a quello necessario agli scopi stessi[33]. La Corte ha, inoltre, precisato che l'obbligo della compagnia assicuratrice di fornire una prova al proprio assicurato dell'avvenuto risarcimento del danno "non può in alcun modo ricomprendere anche la diffusione delle coordinate bancarie delle persone risarcite, atteso che tale trasmissione dei dati oltre a non essere funzionale all'attività per cui gli stessi erano stati raccolti, neppure era necessaria per adempiere al predetto obbligo". *Ex adverso*, infatti, "sarebbe stato sufficiente inviare una comunicazione in cui si dava atto dell'intervenuto ristoro dei danni, come solitamente d'uso nelle compagnie, e/o, al più, consegnargli la quietanza dopo averne debitamente oscurato le informazioni sui dati personali non divulgabili ai sensi della normativa sulla *privacy*". In buona sostanza, l'assicurato avrebbe potuto ricevere una mera comunicazione circa l'avvenuto risarcimento dei danni o, in alternativa, la quietanza con i dati bancari debitamente oscurati[34].

---

32 Il numero iban è certamente un'informazione e in quanto tale esso è usato o sarà probabilmente usato al fine di influire sullo stato di una persona, ad esempio, mediante incremento o decremento della sua ricchezza mobile; inoltre, per le stesse motivazioni l'uso dell'iban ha un impatto sui diritti e sugli interessi di quella persona. Pur se è vero che potrebbe essere relativo a un conto cointestato a più persone, questo non incide sul fatto che l'iban sia un dato personale. Conclusivamente l'iban è un dato personale e ciò discende dalle argomentazioni sopra esposte.

33 Cfr. Cass. Civ., 23 gennaio 2013 n. 1593.

34 Ciò detto, in merito al risarcimento del danno, essendo esclusa la possibilità di subire un pregiudizio di natura patrimoniale in seguito alla illecita diffusione del codice iban, la Suprema Corte ha sancito che il danno risarcibile può consistere anche in quello morale, derivante dal «fastidio, preoccupazione, disagio». Si precisa che, in generale, il risarcimento del danno non patrimoniale non è previsto solo ipso iure come conseguenza di un fatto illecito, ma è dovuto anche nel caso in cui siano stati violati diritti costituzionalmente garantiti. A tal proposito, benché nella nostra Carta fondamentale non ci sia esplicito riferimento alla privacy, essa assurge a rango costituzionale per il viatico dell'art. 2 Cost. il quale riconosce i diritti inviolabili dell'uomo. A tanto aggiungasi che il diritto alla protezione dei dati personali è tutelato non solo dall'anzidetto articolo, ma anche dall'art. 21 Cost., nonché dall'art. 8 Carta dei diritti fondamentali dell'Unione Europea, ai sensi del quale "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano… tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge..". Secondo la Corte, il diritto a mantenere il controllo sulle proprie informazioni, nei diversi contesti ed ambienti di vita, «concorre a delineare l'assetto di una società rispettosa dell'altro e della sua dignità in condizioni di eguaglianza». Chiaramente, non è sufficiente lamentare la lesione del diritto costituzionalmente garantito o affermare l'esistenza del danno, il quale, invece, dovrà essere in ogni caso dimostrato. Pertanto, accertata la sussistenza dell'an di un tale pregiudizio, il giudice adito dovrà

Spetta, quindi, alla banca, in caso di trattamento illecito dei dati personali e per effetto dell'inversione dell'onere probatorio, sotto il profilo della colpa, dimostrare tanto la prova negativa di non aver commesso alcuna violazione delle regole di deontologia e di buona condotta, quanto quella positiva di aver adottato quelle idonee misure preventive di sicurezza, volte a ridurre al minimo i rischi connessi ad un illecito trattamento dei dati[35].

A fronte, infatti, di una violazione della *privacy* del cliente, l'istituto di credito non può essere automaticamente tenuto a risarcire il danno, poiché può sempre dimostrare la mancanza del nesso eziologico tra la condotta (cioè il trattamento dei dati) e l'evento (ossia il danno).

6. Dati particolari (ex dati sensibili) e ipotesi di trattamento lecito in ambito bancario. – L'art. 4, paragrafo 1, del GDPR definisce il dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". All'interno di tale categoria di dato vi è anche quella del dato *particolare* (che il Codice della privacy definiva dato sensibile) inteso come quel dato che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici e biometrici, quelli relativi alla salute, alla vita sessuale o all'orientamento

indagare il quantum debeatur: Cass. Civ., 19 febbraio 2021 n.4475, cit.

35 La violazione di dati personali (o data breach) è una particolare tipologia di incidente di sicurezza che coinvolge dati personali, ossia quelle informazioni che identificano, direttamente o indirettamente, una persona fisica (c.d. interessato). L'art. 4, n. 12, GDPR definisce violazione dei dati personali come "la 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". Le violazioni dei dati personali possono essere classificate in: violazioni della riservatezza, che comportano una divulgazione o un accesso non autorizzato o accidentale ai dati personali; violazioni della disponibilità, che comportano la perdita di accesso o la distruzione accidentali o non autorizzate dei dati personali e violazioni dell'integrità, che comportano una modifica non autorizzata o accidentale dei dati personali.
Esempio di data breach, che può comportare una violazione sia della riservatezza che della disponibilità, è dato dal ransomware, il cui schema è quello dell'estorsione: gli hacker criptano i dati di un'organizzazione e richiedono il pagamento di una somma di denaro (in genere in criptovaluta) per ripristinare l'accesso agli stessi. Spesso l'attacco non si limita alla criptazione dei dati ma consiste anche nella loro esfiltrazione, a cui segue la minaccia di renderli pubblici online in caso di mancato pagamento del riscatto. Ulteriore esempio è dato dal phishing: nella sua versione più semplice, l'hacker, spacciandosi per un'altra persona, invia un'email alla vittima chiedendo di fornire informazioni quali numeri di carte di credito o password. La tecnica di phishing più sofisticata, e che sta prendendo sempre più piede, almeno in Italia, è denominata BEC (Business Email Compromise). In genere, in questo caso l'hacker sottrae le credenziali di accesso all'account email di un dipendente o di un dirigente di un'organizzazione (mediante una normale azione di phishing o introducendosi nei relativi sistemi in altro modo); dopodiché, spacciandosi per un apicale chiede a un proprio dipendente di effettuare un pagamento su un certo conto corrente bancario o, spacciandosi per un fornitore, chiede al committente il pagamento dei corrispettivi dovuti su coordinate bancarie diverse da quelle originariamente comunicate dal reale fornitore. Ed infine, altro esempio di data breach riguarda la perdita di documenti o di dispositivi portatili, nel caso in cui non sia disponibile una copia di backup.

sessuale della persona[36].

Il Regolamento (UE) 2016/679 prevede espressamente una specifica protezione per questa tipologia di dati che, per loro natura, vengono definiti sensibili sotto il profilo dei diritti e delle libertà fondamentali: un trattamento illecito, invero, potrebbe creare rischi significativi per i diritti e le libertà dell'individuo[37]. In generale il GDPR vieta il trattamento di tali dati a tutela e a salvaguardia dell'interessato i cui diritti e le cui libertà fondamentali vanno protetti.

In ambito bancario il trattamento dei dati particolari (ex dati sensibili) viene riconosciuta quando l'interessato ha prestato il proprio consenso (art. 6, paragrafo 1, lettera a), che deve essere informato, cioè deve essere espresso in modo esplicito, chiaro e trasparente e non può essere generalizzato ma deve essere reso per una o più finalità specifiche. La Banca, infatti, per poter trattare tale categoria di dati deve fornire, di volta in volta, all'interessato tutta una serie di informazioni sulla finalità del trattamento: e tante saranno le finalità quante dovranno essere le informazioni rese e i consensi raccolti.

Nel caso in cui la banca intende conservare e/o comunicare a soggetti terzi (per esempio la Società di servizi collegate all'Istituto di Credito) dati personali particolari l'interessato dovrà essere informato della finalità di tali trattamenti e sarà libero di prestare o meno il proprio consenso che, se negato, comporta l'impossibilità per la banca di conservare tali dati e comunicarli a terzi, fatta eccezione per gli obblighi di legge a cui l'Istituto di Credito non può sottrarsi e che possono imporre particolari trattamenti dei dati. Si pensi alla Banca e ai suoi dipendenti: una busta paga può contenere dati particolari sull'appartenenza sindacale (versamento mensile di quota associativa), sulla

---

36 Nel vecchio codice della privacy, all'art.4, comma, 1 lettera d) viene resa la definizione di "dato sensibile": e cioè "i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale". Nel Regolamento europeo, invece, nell'articolo 4 sebbene non esista la definizione di "dato particolare", questo concetto viene espresso successivamente nell'art. 9 "Trattamento di categorie particolari di dati" e precisamente al paragrafo 1: "È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". I dati particolari del GDPR sono i vecchi dati sensibili arricchiti dai dati genetici e quelli biometrici. In dottrina v. F ASTIGGIANO, Illecito trattamento di dati "super sensibili" e risarcimento del danno, in Fam. dir., 2016, 468.

37 Si pensi, ad esempio, in ambito bancario al conto corrente intestato ad un partito politico e le relative movimentazioni effettuate dal tesoriere, a mutui o finanziamenti erogati a persone politicamente esposte, a movimentazioni di denaro da o verso associazioni sindacali, a pagamenti effettuati per prestazioni sanitarie, ad elargizioni di denaro verso movimenti religiosi o verso associazioni a difesa dei diritti di categorie di persone o alla concessione verso i dipendenti dei benefici di cui alla l. n. 104/92.

salute (godimento dei benefici di cui alla legge n. 104/92 per l'assistenza ad un familiare ammalato o disabile). In questi casi la Banca può trattare tali dati perché chiamata ad assolvere obblighi di legge in materia di diritto del lavoro e previdenza sociale purché tali obblighi siano previsti da normative nazionali o comunitarie e dai contratti collettivi nazionali di lavoro[38].

La Banca può, inoltre, trattare i dati particolari del soggetto interessato quando questi siano stati resi manifestamente pubblici dallo stesso interessato. Il trattamento di tali dati è lecito solo ed esclusivamente se necessario al perseguimento delle finalità che la Banca si è posta di raggiungere e che tali finalità devono essere portate a conoscenza degli interessati che devono essere adeguatamente informati.

Altro caso di trattamento lecito di tale categoria di dati si ha quando è necessario per accertare, esercitare o difendere un diritto del titolare del trattamento in sede giudiziaria o ogniqualvolta le Autorità giurisdizionali esercitino le loro funzioni. Quando la Banca, invero, si trova innanzi all'Autorità Giudiziaria per tutelare un proprio diritto, indipendentemente dal fatto che abbia introitato il giudizio o sia stata chiamata a difendersi, può trattare i dati particolari sempre nel rispetto dei principi di necessità e proporzionalità, non eccedendo nel trattamento ma limitandolo alla sola finalità di tutela del proprio diritto in ambito giudiziario. In altre parole, se il cliente della Banca cita in giudizio l'Istituto contestando un rapporto di conto corrente ove sono riscontrabili dati personali particolari, alla Banca sarà consentito il trattamento di tali dati particolari solo ed esclusivamente se funzionali al giudizio e alla tutela del

38 Si v. Cass. Civ., 19 dicembre 2019 n. 34113, per la quale "il trattamento delle informazioni personali effettuato nell'ambito dell'attività di recupero crediti è lecito purché, avvenga nel rispetto del "criterio di minimizzazione" nell'uso dei dati personali, dovendo essere utilizzati solo i dati indispensabili, pertinenti e limitati (non altri elementi ininfluenti) a quanto necessario rispetto alle finalità per cui sono raccolti e trattati. La banca non commette, quindi, alcun illecito né viola la legge sulla privacy solo perché fornisce ad altri soggetti (la società che acquista il credito) informazioni riguardanti il debitore, ma comunque funzionali alla cessione del credito, quali la situazione debitoria e l'ubicazione dell'immobile vincolato alla garanzia del credito. Il trasferimento del database da parte dell'acquirente è ammissibile se la società cedente ha informato gli interessati al trattamento e all'acquisito di uno specifico consenso alla cessione.
Cfr. anche Cass. Civ., 21 ottobre 2019 n. 26778, la quale ha accolto il ricorso di un cliente di una filiale di banca che si è visto bloccare l'operatività del conto corrente a causa della mancata sottoscrizione al consenso per il trattamento dei dati personali sensibili. La Suprema Corte, non condividendo l'impostazione giuridica delle precedenti decisioni, ha osservato che l'obbligatorietà del consenso al trattamento dei dati sensibili contrasta con i principi della legge sulla privacy, che non possono essere derogati all'autonomia privata in quanto posti a tutela di diritti e libertà fondamentali, quali la dignità, la riservatezza, l'identità personale, la protezione dei dati personali. Tra i principi che regolano la tutela della privacy rientra a pieno titolo quello di minimizzazione nell'uso dei dati personali, che impone di utilizzare solo i dati indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati. La Suprema Corte ha così concluso che la clausola con cui la banca subordina l'apertura del conto al consenso al trattamento dei dati sensibili è affetta da nullità in quanto contraria a norme imperative, a norma dell'art. 1418 c.c. Ne consegue che il "blocco" del conto corrente e del deposito titoli, a seguito di una clausola nulla, non esonera la banca da responsabilità per inadempimento contrattuale.

proprio diritto; in caso contrario si avrà un illecito trattamento dei dati.

Ed infine, la Banca può trattare i dati particolari quando ciò si rende necessario per offrire la collaborazione richiesta dalle Autorità giurisdizionali nell'ambito di indagini svolte e più in generale nell'esercizio delle loro funzioni.