CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

Articolo Scientifico

LA TUTELA COMUNITARIA ED ITALIANA DELLA PRIVACY

Il trattamento dei dati personali alla luce del nuovo G.D.P.R. (Regolamento UE n. 2016-679)

di **Pietro Cucumile**
IUS/15 - DIRITTO PROCESSUALE CIVILE
Estratto dal n. 9/2018 - ISSN 2532-9871

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Sabato 22 Settembre 2018

CamminoDiritto.it
ISSN 2532-9871

Sommario: 1. Inquadramento normativo; 2. Le ipotesi di responsabilità civile per il trattamento di dati personali; 3. Il rapporto tra il citato art. 15 D.Lgs. n. 196/03 e l'art. 2059 c.c.; 4. Il diritto all'oblio; 5. Casi di trattamenti di dati pericolosi; 6. Le misure efficaci per una reale protezione dei dati trattati; 7. Conclusioni.

1. Inquadramento normativo.

L'Unione europea, dopo un periodo di studio durato anni, caratterizzato da notizie e anticipazioni, bozze e versioni preliminari in circolazione, ha finalmente emanato il G.D.P.R. (General Data Protection Regulation, Regolamento (UE) 2016/679), normativa complessa e articolata dove è confermato il ruolo centrale del cittadino.

La normativa europea specifica alcuni elementi espressi in termini prima generici e di interesse per questo approfondimento sul trattamento illecito dei dati: la gestione dell'accountability[1], la gestione del data breach, la P.I.A., la ridefinizione di alcune figure specifiche, la positivizzazione della privacy by design[2], la positivizzazione della privacy by default[3].

Inoltre, l'adesione ad un sistema di "certificazione privacy autorizzato" può essere utilizzato per dimostrare la conformità ai requisiti di privacy by design e by default[4]. Come per tutte le certificazioni, però, anche quando l'infrastruttura accreditata sarà disponibile, le conseguenze di un trattamento illecito dei dati non saranno ridotte o trasferite ad altri soggetti, pur se il proprio sistema di gestione della privacy o le figure responsabili ("Data Protection Officer", ecc.) abbiano ottenuto alcune certificazioni.

Da qui si impone un approfondimento della tematica relativa al trattamento illecito dei dati, tenendo ben presente che il modello tendenziale di gestione di un'impresa guarda ad una integrazione di azioni ben resa dall'acronimo G.R.C. (Governance, Risk management e Compliance); queste aree di attività si stanno sempre più allineando e integrando per migliorare le performance dell'impresa e il soddisfacimento dei bisogni degli stakeholder.

Per trattamento si intende un'operazione o complesso di operazioni che abbiano ad oggetto dati personali. Elemento identificativo del trattamento è la finalità, che costituisce lo scopo effettivo per il quale i dati personali siano stati raccolti e gestiti.

La definizione di dato personale era contenuta nell'art. 4 del previgente "Codice Privacy" [5] ed è stata riformulata, con maggiore ricchezza di contenuti, alla voce n° 1 del vigente art. 4 del G.D.P.R.[6]; parimenti, la declaratoria di un trattamento di dati è contenuta alla

CamminoDiritto.it
ISSN 2532-9871

voce n° 2 del vigente art. 4 del G.D.P.R.[7]

In questo seppur breve lavoro si cercherà di sviluppare il ragionamento su alcuni profili dell'istituto del trattamento illecito dei dati, cercando di affrontarlo sia dal punto di vista dell'esegesi normativa che degli orientamenti giurisprudenziali.

A tal fine, partendo dalla lettura del considerando 85 G.D.P.R.[8] si possono così elencare alcuni rischi per l'interessato:

danno morale; discriminazione; diffamazione; pregiudizio alla reputazione; limitazione e perdita di diritti e libertà; assenza di controllo sui propri dati personali; danno fisico; danno economico; furto d'identità; perdita di riservatezza dei dati coperti dal segreto professionale; decifratura non autorizzata della pseudonimizzazione; manifestarsi di effetti giuridici pregiudizievoli a seguito di profilazioni automatizzate. Ebbene, la suprema Corte esclude che la tutela del danno personale assuma carattere assoluto o incondizionato: "il diritto ad esigere una corretta gestione dei propri dati personali, pur se rientrante nei diritti fondamentali di cui all'art. 2 Cost., non è un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale"([9]), sicché le norme sulla tutela dei dati sensibili[10] vanno coordinate e bilanciate con le norme costituzionali che tutelano altri e prevalenti diritti e con le norme ordinarie applicabili al singolo caso concreto.

Aggiunge la suprema Corte: "stabilire dunque se un soggetto pubblico o privato abbia o meno violato le regole legali sulla gestione dei dati altrui impone di interpretare queste ultime bilanciando gli interessi da esse tutelati con gli altri interessi costituzionalmente protetti potenzialmente in conflitto col diritto alla riservatezza"[11].

Parimenti, la Direttiva 95/46/CE non poneva un divieto assoluto e sacrale di uso dei dati, anche sensibili, ma, al contrario, lo consentiva espressamente per l'adempimento di obblighi contrattuali o scaturenti dalla legge e comunque per finalità di interesse pubblico.

Nella medesima prospettiva, il legislatore comunitario specifica, nel nuovo Regolamento europeo sulla protezione dei dati, che "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 contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità".[12]

Colui che tratta dati altrui espone l'interessato ad un rischio ma, attesa l'utilità generale alla circolazione dei dati, l'attività di trattamento è ritenuta lecita ancorché limitata dalla

CamminoDiritto.it
ISSN 2532-9871

necessità di adottare un sistema rigoroso di sicurezza e di protezioni, oltre che di responsabilità.

L'intera normativa nazionale è volta ad evitare che i dati personali siano trattati in modo da cagionare danni ai soggetti a cui i dati stessi si riferiscono: sia gli strumenti preventivi veri e propri [13] che l'ampia operatività del regime di responsabilità civile sono iscritti in una logica preventiva e dissuasiva.

2. Le ipotesi di responsabilità civile per il trattamento di dati personali.

Disciplinando le **ipotesi di responsabilità civile** connesse al trattamento dei dati personali mediante il combinato disposto degli artt. 15 D.Lgs. n. 196/03 e 2050 c.c., il legislatore nazionale ha predisposto una tutela rafforzata e tendenzialmente esaustiva dei soggetti danneggiati dalle operazioni di trattamento dei dati, aggiungendo agli strumenti a carattere preventivo il tradizionale rimedio risarcitorio e rafforzando quest'ultimo mediante la predisposizione di un regime di responsabilità civile aggravata[14].

La giurisprudenza di legittimità non indugia sulla natura della responsabilità civile per illecito trattamento dei dati personali e, anche nei casi in cui si soffermi, incidentalmente, sul tema, concentra l'attenzione sull'onere della prova e sul nesso di causalità: "i danni cagionati per effetto del trattamento dei dati personali in base all'art. 15, D.Lgs. n. 196 del 2003, sono assoggettati alla disciplina di cui all'art. 2050 c.c., con la conseguenza che il danneggiato è tenuto solo a provare il danno e il nesso di causalità con l'attività di trattamento dei dati, mentre spetta al convenuto la prova di aver adottato tutte le misure idonee ad evitare il danno"**[15]**.

Ancora: "… ricostruita in termini di colpa presunta o di responsabilità oggettiva, non vi è dubbio che l'affermazione della responsabilità dell'esercente l'attività pericolosa, ai sensi dell'art. 2050 c.c., richieda comunque l'accertamento della sussistenza di un nesso di causalità tra l'attività e il danno patito dal terzo …"[16].

Sebbene la giurisprudenza italiana non assuma una posizione univoca in merito alla natura pericolosa delle operazioni di trattamento dei dati[17], il ragionamento di quella più sensibile al tema può trovare rappresentazione nel passo qui di seguito riprodotto:

"Il diritto alla riservatezza (o all'intimità della sfera privata dell'individuo) appare, ben più di altri aspetti di tutela della personalità, strettamente collegato alle profonde trasformazioni operate dalla società industriale e post-industriale: accresciuto contatto e ad un tempo maggiore estraneità tra gli individui, più ampio dinamismo e circolazione dei

CamminoDiritto.it
ISSN 2532-9871

soggetti, che possono inserirsi in ambienti e situazioni tra loro del tutto indipendenti, talora rivestendo ruoli differenziati e mostrando così profili diversi della propria personalità. **E', poi, soprattutto l'incessante progresso tecnologico, con il perfezionamento (e la pericolosità) dei mezzi di comunicazione di massa e degli strumenti di raccolta di dati e notizie che, attraverso inedite, per il passato del tutto impensabili, e talora gravissime, aggressioni agli aspetti più intimi della personalità, richiede necessariamente l'individuazione di più adeguate ed efficaci difese**"[18].

In base alla normativa europea, il titolare risponde anche soltanto per non avere adottato tutte le misure idonee di sicurezza e per non averle efficacemente **documentate**. La responsabilità derivante dall'illecito trattamento dei dati riguarda tutti i profili del trattamento e, segnatamente, il rispetto delle norme, giuridiche e tecniche, relative alle modalità e finalità del trattamento,sicché i titolari del trattamento: sono responsabili della conformità delle operazioni compiute alla normativa in materia di protezione dei dati personali, devono adottare tutte le misure idonee a garantire la protezione dei dati trattati e devono essere in grado di dimostrare, in qualunque momento, tale idoneità.

Il principio, costantemente ribadito nei pareri del Gruppo art. 29[19] informa il Regolamento U.E. n. 2016/679 fondato sulla "responsabilizzazione" (accontaubility) dei titolari e dei responsabili[20].

3. Il rapporto tra il citato art. 15 D.Lgs. n. 196/03 e l'art. 2059 c.c.

Il sistema normativo di responsabilità civile delineato nel D.Lgs. n. 196/03, imperniato sul relativo art. 15, impone l'esame di due, connessi, aspetti problematici: il significato da attribuire al rinvio, contenuto nel primo comma della citata norma, all'art. 2050 c.c.; il rapporto tra il citato art. 15 e l'art. 2059 c.c., implicante, in virtù del secondo comma, l'estensione della tradizionale area di risarcibilità del danno non patrimoniale.

In merito al danno non patrimoniale risarcibile ai sensi dell'art. 15 del D.Lgs. n. 196/03, la giurisprudenza è ormai pervenuta ad una consolidata opinione: sebbene costituisca una lesione del diritto fondamentale alla protezione dei dati personali, tale danno presuppone la verifica della "gravità della lesione" e della "serietà del danno"; la risarcibilità del danno derivante dall'illecito trattamento di dati personali è condizionata al superamento di una soglia minima di tollerabilità ed il relativo pregiudizio, ancorché inquadrato nelle ipotesi di lesioni di diritti costituzionalmente garantiti, deve essere provato, indipendentemente dall'entità e dalla difficoltà di assolvere l'onere probatorio, secondo le regole ordinarie, **trattandosi di un danno-conseguenza e non di un danno evento.**

In ordine al rinvio dell'art. 15 D.Lgs. n. 196/03 all'art. 2050 c.c. si registrano due diverse

CamminoDiritto.it
ISSN 2532-9871

linee interpretative. In base ad una prima opzione, l'art. 15 avrebbe qualificato **in termini di pericolosità l'attività di trattamento dei dati** al fine di favorire, nel settore dei dati personali, l'applicabilità del relativo regime codicistico di responsabilità.

Questa ricostruzione, volta a qualificare come pericolosa l'attività di trattamento dei dati, valorizza le esigenze di tutela dei diritti fondamentali della persona e la conseguente pericolosità della loro lesione. Un diverso orientamento afferma che il riferimento all'art. 2050 c.c. costituirebbe un mero rinvio alla regola probatoria contenuta in questa norma: il danneggiante sarebbe gravato dalla prova liberatoria prevista nell'art. 2050 c.c. e le operazioni di trattamento dei dati non sarebbero, di per sé, "pericolose".

La prima prospettiva escluderebbe, secondo parte della dottrina, la sussistenza di una disciplina autonoma in materia di trattamento illecito dei dati, implicando, in virtù del mero rinvio operato dall'art. 15, l'applicazione diretta dell'intero contenuto dell'art. 2050 c.c..

Il secondo indirizzo interpretativo troverebbe giustificazione in plurimi argomenti: la mera necessità di agevolare l'onere probatorio posto a carico del danneggiato in un settore caratterizzato dall'incessante evoluzione tecnologica; l'impossibilità, d'intuitiva evidenza, di ritenere che ogni trattamento dei dati costituisca attività pericolosa.

Sotto il profilo operativo-funzionale la pericolosità o meno delle attività di trattamento appare una questione terminologica, operando, in ogni caso, in favore del danneggiato, la facilitazione probatoria di cui al combinato disposto degli artt. 15 del D.Lgs. 196/03 e 2050 c.c. e gravando, comunque, sul danneggiante la rigorosa prova liberatoria "di avere adottato tutte le misure idonee a evitare il danno".

La giurisprudenza ritiene sufficiente, per accertare la sussistenza della responsabilità ai sensi dell'art. 2050 c.c., che il danneggiato provi "l'evento di danno e il nesso di causalità tra l'attività ed esso, spettando invece all'esercente dimostrare di avere adottato tutte le misure idonee ad evitare il danno".

La formulazione letterale dell'art. 15 del D.Lgs. n. 196/03 e le incertezze interpretative in merito al suo ambito applicativo hanno indotto a riflettere in ordine all'individuazione **dell'interesse protetto** in relazione alle diverse tipologie e modalità del trattamento.

Secondo un primo orientamento, il legislatore avrebbe introdotto una disciplina "procedimentale" posta a tutela della **sola legittimità del trattamento**, di talché ogni attività di trattamento effettuata in violazione dei principi e delle prescrizioni del Codice

CamminoDiritto.it
ISSN 2532-9871

di protezione dei dati personali, cagionando un pregiudizio al bilanciamento di interessi effettuato in sede normativa, legittimerebbe il ricorso al rimedio risarcitorio.

Secondo un'altra prospettiva, posto che il D.Lgs. n. 196/03 non consente una protezione assoluta ed incondizionata di ogni istanza di tutela, garantendo, invece, il giusto punto di equilibrio, sancito ex ante dal legislatore, tra i diversi diritti ed interessi in gioco, la mera violazione procedurale[21], non giustificherebbe di per sé l'ammissibilità del rimedio risarcitorio. Sarebbe indispensabile l'individuazione di un danno ingiusto consistente nella lesione di un diritto riconducibile all'interessato[22], sicché il comportamento antigiuridico legittimerebbe l'azione risarcitoria solo in caso di pregiudizio a situazioni giuridiche soggettive rilevanti per l'interessato. L'interesse tutelato dalla norma non sarebbe quello meramente procedurale al trattamento conforme alla legge, dovendo concretizzarsi, invece, nella tutela dei diritti fondamentali della persona.

La disamina dei contrasti dottrinali in relazione agli interessi protetti ed alle situazioni soggettive ammesse alla tutela risarcitoria rende ancora più evidente l'esigenza della concreta individuazione delle situazioni soggettive ammesse alla tutela risarcitoria.

4. Il diritto all'oblio.

Dunque, occorre individuare, innanzitutto, le situazioni soggettive ammesse al risarcimento e verificando, in secondo luogo, la sussumibilità di tali fattispecie nel regime applicativo specifico dell'art. 2050 c.c..

Ebbene, **in punto di diritto all'oblio**, la ricerca del difficile equilibrio tra diritti della personalità e diritto dell'informazione al fine di valutare la liceità o illiceità dei trattamenti in ragione del trascorre del tempo deve modularsi in base al mezzo di comunicazione di massa che acquisisce o rende pubblica la notizia.

Il bene giuridico tutelato è sempre quello dell'identità personale che, ove si valuti la dialettica tra il diritto all'oblio e l'interesse dei motori di ricerca, va bilanciato con altri diritti costituzionali e diritti fondamentali dell'Unione europea: libertà di informazione, di espressione, di accessibilità universale alle informazioni su internet, d'impresa.

Del "diritto all'oblio", concepito come nuovo profilo del diritto alla riservatezza, valutato in relazione all'attualità dell'interesse pubblico all'informazione, giurisprudenza e dottrina hanno fornito molteplici e non conformi definizioni.

Il diritto all'oblio, più che un autonomo diritto della personalità, viene considerato "un

CamminoDiritto.it
ISSN 2532-9871

aspetto del diritto all'identità personale, segnatamente il diritto alla **dis-associazione** del proprio nome da un dato risultato di ricerca"[23].

Il ridimensionamento della propria visibilità telematica rappresenta un aspetto funzionale del diritto all'identità personale[24], implicante la valutazione di contrapposti interessi: quello dell'individuo a non essere più trovato on-line, quello del motore di ricerca alla libertà di iniziativa economica e quello degli utenti di internet all'informazione[25].

Dunque, l'esigenza di attribuzione della fonte dell'informazione ad un soggetto e la necessità di garantire la qualità e la correttezza dell'informazione impongono il superamento del criterio dell'attualità dell'interesse pubblico all'informazione, considerato dalla risalente giurisprudenza elemento costitutivo del diritto all'oblio, a favore dell'applicazione delle norme del D.Lgs. n. 196/03, inteso come "statuto generale dei diritti della persona, idoneo a portare a compimento una sorta di eugenetica capillare dei diritti della personalità".

Le controversie aventi ad oggetto il diritto alla deindicizzazione devono essere correttamente inquadrate, indipendentemente dall'assimilazione al "diritto all'oblio", nell'ambito della disciplina relativa al trattamento dei dati personali[26].

La giurisprudenza nazionale, esaminato il vigente quadro normativo nazionale, rinviene la disciplina del diritto all'oblio negli artt. 7,11 e 25 del "Codice della privacy". Le norme contenute nel D.Lgs. n. 196/03 perseguono, infatti, l'obiettivo di garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità dell'interessato con particolare riferimento al diritto alla riservatezza.

In particolare, l'art. 11 prevede che il trattamento dei dati personali sia effettuato per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati erano stati raccolti e trattati, **l'art. 25 vieta la comunicazione e la diffusione dei dati ove sia decorso il periodo di tempo indicato nell'art. 11** e l'art. 7 attribuisce all'interessato il diritto di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge[27]. Pertanto, l'illecito protrarsi del trattamento dei dati personali che sia inquadrabile all'interno di questo perimetro normativo giustifica l'accertamento della responsabilità civile ai sensi degli artt. 15 D.lgs. n. 196/03 e 2050 c.c. [28].

5. Casi di trattamenti di dati pericolosi.

Il persistere del trattamento dei dati personali e il decorso del tempo sufficiente alla

CamminoDiritto.it
ISSN 2532-9871

soddisfazione dell'interesse pubblico alla divulgazione delle notizie, ove cagioni la lesione dei diritti dell'interessato alla riservatezza e alla reputazione, legittima la tutela dei diritti alla cancellazione e/o alla rettifica dei dati ed al risarcimento dei danni subiti ai sensi degli artt. 11 e 15 del D.Lgs. n. 196/03.

L'art. 17 del nuovo Regolamento europeo richiama i requisiti del decorrere del tempo ed alla sopravvenuta **superfluità dei dati rispetto alle finalità** per le quali sono stati raccolti e trattati (art. 17, par. 1, lett. a) nonché dell'intervenuta revoca del consenso (art. 17, par. 1, lett. b).

Non può ritenersi che le precedenti elaborazioni siano superate dal paragrafo 2 dell'art. 17, secondo il quale il titolare del trattamento, se ha reso pubblici i dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, ha l'obbligo di informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato "di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

La giurisprudenza considera pericolose le operazioni di trattamento dei dati che, relative a persone arrestate o anche sottoposte a particolari esami clinici, possono cagionare una consistente lesione alla dignità della persona. In tal senso, risalente giurisprudenza di merito ha rilevato che costituisce illegittimo trattamento di dati personali, in base all'art. 2050 c.c., la pubblicazione su un quotidiano della c.d. "fotografia emblematica", ritraente una persona sottoposta ad un **esame etilometrico** da parte della polizia stradale: la pubblicazione del dato personale non poteva ritenersi essenziale rispetto all'interesse pubblico alla relativa informazione sicché l'identità del danneggiato era stata rivelata in mancanza di un valido motivo giornalistico da portare a conoscenza della comunità. Il Tribunale, dunque, condannava al risarcimento del danno per violazione della disciplina in materia di trattamento dei dati personali l'editore del quotidiano, responsabile per avere pubblicato la fotografia che ritraeva il soggetto, facilmente riconoscibile, mentre si sottoponeva all'esame alcolimetrico, effettuato dagli agenti della polizia stradale[29]. La peculiare condizione di vulnerabilità della persona sottoposta ad arresto o ad esami clinici, potenzialmente esposta ad un irreversibile pregiudizio della propria reputazione, immagine e dignità, avvalora, invero, l'applicabilità del più rigoroso regime di responsabilità di cui all'art. 2050 c.c.

La Corte di legittimità, in tema di diritto alla riservatezza di un **minore affetto da disabilità**, ha rilevato che l'immediata percepibilità da parte di terzi della condizione di disabilità non può considerarsi fatto reso noto direttamente dall'interessato o attraverso un comportamento di questi in pubblico e che conseguentemente risulta violata la riservatezza di una minore della quale siano divulgati gli elementi di identificazione e i dati sensibili attinenti alla sua salute, senza che essi fossero, peraltro, di interesse pubblico

CamminoDiritto.it
ISSN 2532-9871

ed essenziali all'informazione. La suprema Corte, dunque, confermava la sentenza di merito che aveva ritenuto risarcibile, ai sensi degli artt. 11 e 15 del Codice della privacy, i danni cagionati dall'illegittima divulgazione di una delibera comunale di assistenza di un minore diversamente abile, corredata dell'indicazione del nome e cognome dell'interessato[30].

La sentenza riteneva costituire un'ulteriore conferma della sussistenza della responsabilità civile, la possibilità, per colui che compie operazioni di trattamento di dati già pubblici o pubblicati, del loro accostamento, comparazione, esame, analisi, congiunzione, rapporto o incrocio, ricavando un "valore aggiunto informativo", non estraibile dai dati isolatamente considerati, potenzialmente lesivo della dignità dell'interessato.

Si registra un contrasto, nella giurisprudenza di merito, in ordine alla riconducibilità delle fattispecie illecite costituite **dall'erronea segnalazione di un soggetto nella Centrale rischi della Banca d'Italia** al regime normativo di protezione dei dati personali: alcune pronunce applicano il combinato disposto degli artt. 2050 c.c. e 15 D.Lgs. n. 196/03[31] mentre altre richiamano la normativa di settore (l. n. 386/90) ed il rispetto dei principi generali in tema di correttezza e buona fede, senza alcun riferimento alla normativa di tutela dei dati personali[32].

La giurisprudenza di legittimità ritiene decisiva, ai fini dell'assoggettamento delle controversie risarcitorie alla disciplina di cui al D.Lgs. n. 196/03, la derivazione causale dell'illecito dal trattamento dei dati personali da parte del suo titolare[33]. In particolare, la suprema Corte afferma che la Banca d'Italia, in relazione al trattamento dei dati personali effettuato dalla Centrale Rischi, non è estranea all'applicazione del "Codice privacy", con conseguente applicabilità delle norme generali in tema di trattamento dei dati di cui all'art. 11: "nella gestione della centrale dei rischi, la Banca d'Italia non si sottrae alla disciplina generale in tema di trattamento dei dati personali, dettata dal d.lgs. n. 196/03 (…) è pertanto configurabile una responsabilità civile della Banca d'Italia in relazione ai danni cagionati dal predetto trattamento, ai sensi dell'art. 11 D.Lgs. n. 196/03"[34].

Proposto ricorso ex art. 152 D.Lgs. n. 196/03, la Corte di Cassazione accoglieva il ricorso, rilevando, invece, l'inutilizzabilità dei dati personali trattati in violazione della disciplina di cui al "Codice privacy" e la responsabilità civile per i danni cagionati per effetto del trattamento ai sensi degli artt. 15 D.Lgs. n. 196/03 e 2050 c.c..

La suprema Corte, rilevato che l'annotazione del nominativo presso le banche dati private rientra nell'ambito di applicazione del D.Lgs. 30 giugno 2003, n. 196, art. 11, dovendo i dati personali essere "trattati in modo lecito e secondo correttezza" e rispondere a requisiti di esattezza e di aggiornamento, riteneva che la decisione impugnata, evidenziando che la

CamminoDiritto.it
ISSN 2532-9871

resistente aveva tenuto "una condotta volta ad evitare danno alcuno", aveva valutato, pur senza enunciare formalmente il canone della responsabilità di cui all'art. 2050 c.c., il comportamento tenuto dal gestore dei dati personali "alla stregua dei principi ricavabili dalla norma citata".

In un successivo, più recente, arresto i giudici di legittimità hanno espresso un diverso orientamento quanto alla natura della responsabilità ex art. 2050 c.c.[35].

Convenute in giudizio dinanzi al Tribunale, ai sensi dell'art. 152 D.Lgs. n. 196 del 2003, la banca segnalante e la Banca d'Italia, l'istante chiedeva disporsi l'immediata cancellazione del suo nominativo dalla Centrale Rischi, categoria "sofferenze", ivi inserito a seguito di illegittima segnalazione, oltre al risarcimento dei danni e alle spese. Il ricorrente denunciava la violazione del combinato disposto degli artt. 2050 c.c. e 15 D.Lgs. n. 196/03, sostenendo che il Tribunale, una volta riconosciuta l'illegittimità della segnalazione a sofferenza, avrebbe dovuto condannare la Banca segnalante al risarcimento dei danni, in applicazione dell'art. 2050 c.c., ponendo esso una fattispecie di responsabilità oggettiva e dovendosi considerare il danno, ivi compreso quello all'immagine e alla reputazione, in re ipsa.

La suprema Corte precisava che la responsabilità per attività pericolosa di cui all'art. 2050 c.c. non costituisce, alla luce della giurisprudenza di legittimità, un'ipotesi di responsabilità oggettiva: l'indirizzo prevalente, argomentando dalla prova liberatoria prevista dalla norma e dalla Relazione al codice civile, ricostruirebbe la responsabilità dell'esercente l'attività pericolosa in termini di colpa presunta mentre sarebbe minoritario l'orientamento volto ad inquadrare la responsabilità per l'esercizio di attività pericolose nell'ambito della responsabilità oggettiva. In ogni caso, la responsabilità prevista nell'art. 2050 c.c. richiederebbe comunque l'accertamento della sussistenza di un nesso di causalità tra l'attività e il danno patito dal terzo e dunque l'esistenza di un danno che il Tribunale correttamente aveva ritenuto non provato[36].

La cifratura dei dati, negli adempimenti previsti per comunicazioni e notificazioni, costituisce una delle misure minime idonee ad impedire il danno, sicché l'omessa attuazione di tale accorgimento obbliga chi compie l'attività di trattamento di tali dati, da considerarsi pericolosa ai sensi dell'art. 2050 c.c., al relativo risarcimento. Applicando questi principi, la suprema Corte ha cassato la sentenza di merito che aveva escluso la responsabilità di un Ente regionale e di un istituto bancario per avere contribuito alla diffusione di un dato sensibile di un correntista, costituito dal riferimento alla legge n. 210 del 25/02/1992 che riconosce un indennizzo a chi abbia riportato, a causa di vaccinazioni obbligatorie, una menomazione permanente all'integrità psicofisica o a chi risulti contagiato da infezioni HIV a seguito di somministrazione di sangue o derivati. L'istante

CamminoDiritto.it
ISSN 2532-9871

aveva convenuto in giudizio la banca e l'ente pubblico per una diffusione illecita di dati sensibili, a seguito dell'indicazione, nell'ordine di bonifico e nel conto corrente, della causale dell'indennizzo di un danno alla salute; la Regione aveva trasmesso il dato e la banca lo aveva riportato nell'estratto conto quale causale del bonifico disposto in suo favore.

Di più, i dati sensibili idonei a rilevare **lo stato di salute** della persona possono essere trattati solo se cifrati o criptati in modo da rendere non identificabile il soggetto interessato. Pertanto, i soggetti, pubblici o privati, ancorché agiscano in funzione o con finalità di pubblico interesse, devono osservare tali cautele[37].

Sempre, in merito al trattamento ad opera della pubblica amministrazione di dati personali e sensibili, il supremo Collegio ha confermato la sentenza di merito che aveva condannato un Comune ed un suo dirigente, responsabili per l'affissione di un documento relativo alla richiesta **di riconoscimento della causa di servizio per una patologia**[38], rigettando le censure proposte in sede di legittimità, relative alla pretesa violazione degli artt. 15 D.Lgs. n. 196/03, 2050, 2059 e 2697 c.c..

La pubblicazione sull'albo pretorio, avvenuta con modalità tali da far conoscere la patologia a chiunque avesse esaminato il contenuto della bacheca comunale, aveva cagionato danni risarcibili, consistenti nel disagio, nell'imbarazzo e nella preoccupazione determinatisi in capo al dipendente danneggiato. La pubblicazione della determinazione amministrativa, infatti, era avvenuta con modalità (affissione del documento, contenente dati sensibili e visibile a tutti) idonee a violare il diritto alla riservatezza (chiunque avrebbe potuto apprendere le informazioni sulla salute del soggetto interessato) e, in particolare, il principio di pertinenza e della non eccedenza di cui all'art. 11 del "Codice privacy".

Integra, altresì, gli estremi del trattamento illecito dei dati personali la condotta di un Comune che, dopo aver tentato, con esito negativo, di notificare, a mezzo posta, un'ordinanza-ingiunzione emessa nel procedimento di applicazione di una sanzione amministrativa comminata al soggetto che, in violazione di un'ordinanza sindacale, si era fermato per consentire la salita sul proprio veicolo a una persona dedita **all'attività di prostituzione**, si sia avvalso, a tal fine, dei messi del Comune dove l'interessato abitava i quali recapitavano il plico, non in busta chiusa, presso la residenza dell'ingiunto e a mani di sua madre[39]. Il comportamento del Comune, che non si era avvalso della notificazione presso il domicilio eletto costituiva una condotta integrante l'illecito trattamento di dati personali, come tale riconducibile alla fattispecie risarcitoria di cui all'art. 15 D.Lgs. n. 196/03. Quale titolare del trattamento di dati personali, il Comune avrebbe dovuto gestire la pratica amministrativa in relazione al contenuto della violazione contestata, esperendo,

CamminoDiritto.it
ISSN 2532-9871

prima di ricorrere ai messi, la notificazione al domicilio eletto. Decidendo di non praticare la forma di notifica presso il domicilio legale eletto, l'Ente non aveva "adottato tutte le misure idonee ad evitare il danno" e, dunque, non aveva fornito, ai sensi dell'art. 2050 c.c., la prova liberatoria relativa all'illegittimo trattamento dei dati.

In ordine ai danni cagionati per effetto del trattamento dei dati personali in **ambito condominiale**, la suprema Corte afferma il principio che, ove vi sia stata una divulgazione di dati personali non si realizza necessariamente una violazione della relativa legge, dovendosi comunque effettuare una comparazione tra gli interessi coinvolti. Pertanto, esclude che la divulgazione di dati personali non contenuti in un documento condominiale, bensì in una lettera privata spedita dai ricorrenti all'amministratore condominiale, relativa all'esistenza dell'iniziativa privata di costruzione di un ascensore, costituisca un comportamento lesivo della privacy. La condotta dell'amministratore condominiale che, anziché limitarsi a riferire la notizia, aveva spedito a tutti i condomini una fotocopia della documentazione riservata ricevuta in visione, non costituiva una violazione della privacy degli interessati ma, al contrario, un atto dovuto nell'ambito dei compiti e delle funzioni proprie dell'amministratore, rispondente alle esigenze della legittima e doverosa esecuzione del mandato[40].

Il supremo Collegio ritiene, inoltre, che costituisca illecita diffusione di dati personali, fonte di responsabilità civile ai sensi degli art. 11 e 15 D.Lgs. n° 196/2003, l'affissione, ad opera dell'amministratore, nella bacheca dell'androne dell'edificio condominiale, ovvero in un luogo aperto all'accesso a terzi estranei al condominio, dell'informazione concernente **le posizioni di debito dei singoli partecipanti al condominio** in ordine all'onere di contribuzione alle spese comuni"[41]. La sentenza impugnata era errata nella parte in cui aveva ritenuto prevalenti, sul diritto alla riservatezza, "esigenze di efficienza", effettuando un bilanciamento che non teneva conto del rango di diritto fondamentale assunto dal diritto alla protezione dei dati personali.

Il trattamento dei dati personali, per essere lecito, deve avvenire nell'osservanza dei principi di proporzionalità, di pertinenza e di non eccedenza rispetto agli scopi per i quali i dati stessi sono raccolti (art. 11 del codice); sull'amministratore del condominio, pertanto, grava il dovere di adottare "le opportune cautele per evitare l'accesso a quei dati da parte di persone estranee al condominio"[42].

Le pronunce che ascrivono **agli intermediari bancari e finanziari la responsabilità extracontrattuale** derivante dall'esercizio di attività pericolosa seguono il medesimo iter logico-giuridico: richiamati l'art. 15 e l'art. 31 del D.Lgs. n. 196/03, imputano all'istituto bancario, quale titolare del trattamento dei dati personali, il danno provocato al risparmiatore per non avere predisposto le misure di sicurezza idonee ad impedire

CamminoDiritto.it
ISSN 2532-9871

l'illecito accesso di terzi al sistema di home banking.

Si registrano, nell'ambito di tale iter argomentativo, significative varianti: alcune decisioni sovrappongono le valutazioni inerenti alla responsabilità extracontrattuale, evinta dagli artt. 15 e 31 D.Lgs. n. 196/03 e 2050 c.c., a quelle relative alla responsabilità contrattuale, ricondotta all'art. 1176 c.c.[43]; altre pervengono alla condanna dell'istituto bancario anche in mancanza di accertamenti tecnici che individuino, con ragionevole certezza, il nesso di causalità[44]; altre, infine, pur invocando il regime di responsabilità da attività pericolosa, attribuiscono alle banche una responsabilità per colpa, eludendo la prevalente giurisprudenza orientata nel senso della natura oggettiva della responsabilità ex art. 2050 c.c.[45].

Per contro, le sentenze che escludono l'inquadramento della responsabilità civile per danno da "phishing" dall'ambito applicativo dell'art. 2050 c.c. non aderiscono ai principi che ormai costituiscono diritto vivente in tema di responsabilità per esercizio di attività pericolose[46].

Secondo la suprema Corte[47]: «Né si può escludere che in futuro - con il moltiplicarsi del numero e della potenzialità dannosa degli illeciti - possano essere elaborate regole peculiari e più ampie di imputazione della responsabilità, a tutela degli utenti dei servizi bancari»[48].

In una recente pronuncia, la suprema Corte ha affermato la responsabilità dell'istituto bancario per inosservanza della diligenza dallo stesso esigibile: "In tema di ripartizione dell'onere della prova, al correntista abilitato a svolgere operazioni "on line" che, alla stregua degli artt. 15 del d.lgs. n. 196 del 2003 e 2050 c.c., agisca per l'abusiva utilizzazione (nella specie, mediante illegittime disposizioni di bonifico) delle sue credenziali informatiche, spetta soltanto la prova del danno siccome riferibile al trattamento del suo dato personale, mentre l'istituto creditizio risponde, quale titolare del trattamento del dato, dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico mediante la captazione dei codici d'accesso del correntista, ove non dimostri che l'evento dannoso non gli sia imputabile perché discendente da trascuratezza, errore o frode del correntista o da forza maggiore"[49].

La sentenza conferma, in definitiva, il precedente orientamento secondo il quale "il mancato rispetto dell'obbligo del titolare della carta di chiederne immediatamente il blocco, nei casi di sottrazione o smarrimento, non esime necessariamente da responsabilità il banchiere, allorquando la carta viene "catturata" dall'apparecchio ATM a causa di una manomissione"[50].

CamminoDiritto.it
ISSN 2532-9871

In favore dell'applicabilità degli artt. 15 D.Lgs. n. 196/03 e 2050 c.c. alle ipotesi di danni derivanti dall'attività di fornitura del sistema di home banking alla clientela, depongono ulteriori argomenti, di ordine teorico, normativo e sistematico.

L'illecita percezione delle somme custodite mediante l'home banking è sempre preceduta, nei casi di phishing, dall'accesso abusivo a dati "personali", intaccando interessi non esclusivamente patrimoniali e legittimando l'applicazione dell'art. 15 "Codice della privacy".

In punto di gravità della lesione e della serietà del danno la suprema Corte così si esprime [51]:

"Il danno non patrimoniale risarcibile ai sensi dell'art. 15 d.lgs. 30 giugno 2003 n. 196 non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" che, in linea generale, si richiede ex art. 2059 c.c. nelle ipotesi di pregiudizio inferto ai diritti inviolabili di rilevanza costituzionale: anche nelle fattispecie di danno morale opera il bilanciamento del diritto tutelato da tale norma con il principio di solidarietà - di cui il principio di tolleranza è intrinseco precipitato -, principio che permette di salvaguardare il diritto del singolo nell'ambito di una concreta comunità di persone che deve affrontare i costi di una coesistenza collettiva. L'accertamento di fatto, rimesso al giudice del merito, dovrà essere ancorato alla concretezza della vicenda materiale portata alla cognizione giudiziale ed al suo essere maturata in un dato contesto temporale e sociale, dovendo l'indagine proiettarsi sugli aspetti contingenti dell'offesa e sulla singolarità delle perdite personali verificatesi: siffatto accertamento, che, ove l'offesa non superi la minima tollerabilità o il danno sia futile, può anche escludere un risarcimento, è, come tale, sottratto al sindacato di legittimità se congruamente motivato. La violazione dell'art. 11 - in quanto la norma è volta a delineare i criteri di comportamento, lecito e corretto, ai quali si deve conformare il titolare o il responsabile del trattamento dei dati personali - non assorbe in sè tutte le componenti materiali dell'illecito, mentre l'art. 15, sia pure non aggettivandolo come ingiusto, indica in ogni caso la necessità dell'esistenza di un danno che sia effetto di un trattamento di dati personali. Tale rilievo è da coniugare con l'ulteriore considerazione – fatta propria dalla giurisprudenza di questa Corte - secondo cui la tutela apprestata dal codice della privacy al diritto alla protezione dei dati personali non è espressione di una concezione "statica" della riservatezza, bensì "dinamica" di essa, "tesa al controllo dell'utilizzo e del destino dei dati"[52]. Tale evoluzione esalta le finalità rispetto alle quali è improntato il sistema delineato dallo stesso decreto, in cui diventa prioritaria la tutela "dei diritti e delle libertà fondamentali e della dignità della persona, e in particolare della riservatezza" e, per l'appunto, "del diritto alla protezione dei dati personali nonchè dell'identità personale o morale del soggetto", indicati dall'art. 2 del codice (tra le molte, oltre alla già citata Cass. n. 17602 del 2013, anche Cass., 8 agosto 2013, n. 18981 e, in precedenza, Cass., 8 luglio 2005, n. 14390). Di qui, la necessità di un

CamminoDiritto.it
ISSN 2532-9871

bilanciamento tra contrapposti diritti e libertà fondamentali, in cui, seppur senza posizioni gerarchicamente definite, dovrà trovare adeguata considerazione anche il diritto fondamentale "alla protezione dei dati personali, tutelato agli artt. 21 e 2 Cost., nonchè all'art. 8 Carta dei diritti fondamentali dell'U.E., quale diritto a mantenere il controllo sulle proprie informazioni che, spettando a chiunque (D.Lgs. n. 196 del 2003, art. 1) e ad ogni persona (art. 8 Carta), 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"[53].

In punto, invece, di nesso di causalità e di prova liberatoria la suprema Corte afferma che [54]: "In riferimento all'art. 2050 c.c., la giurisprudenza di questa Corte è consolidata nell'affermare il seguente principio di diritto: "In tema di illecito aquiliano, perchè rilevi il nesso di causalità tra un antecedente e l'evento lesivo deve ricorrere la duplice condizione che si tratti di un antecedente necessario dell'evento, (nel senso che questo rientri tra le conseguenze normali ed ordinarie del fatto), e che l'antecedente medesimo non sia poi neutralizzato, sul piano eziologico, dalla sopravvenienza di un fatto di per sè idoneo a determinare l'evento. Ne consegue che, anche nell'ipotesi in cui l'esercente dell'attività pericolosa non abbia adottato tutte le misure idonee ad evitare il danno, realizzando quindi una situazione astrattamente idonea a fondare una sua responsabilità ex art. 2050 c.c., la causa efficiente sopravvenuta che abbia i requisiti del caso fortuito (eccezionalità ed oggettiva imprevedibilità) e sia idonea, da sola, a causare l'evento, recide il nesso eziologico tra quest'ultimo e l'attività pericolosa, producendo effetti liberatori anche quando sia attribuibile al fatto del danneggiato stesso o di un terzo".

Ancora, secondo la suprema Corte[55]:

"La statuizione di non luogo a provvedere assunta dall'Autorità Garante per la protezione dei dati personali ex art. 149, comma 2, del d.lgs. 30 giugno 2003, n. 196, derivante dall'adesione spontanea da parte del titolare del trattamento alla cancellazione e non utilizzazione di dati, così come richiesto dagli interessati, non impedisce l'esercizio dell'azione di risarcimento del danno davanti all'autorità giudiziaria ordinaria; nè tale azione deve essere proposta nel termine perentorio di trenta giorni dalla comunicazione del provvedimento del Garante. I provvedimenti che possono essere adottati dal Garante, su ricorso proposto ai sensi del D.Lgs. n. 196 del 2003, ex art. 141, lett. c), si articolano in misure di natura provvisoria e definitiva. Tra i primi vi sono il blocco in tutto od in parte dei dati o la sospensione del trattamento. In ordine ai provvedimenti definitivi il Garante può disporre la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. Se richiesto dalle parti, il Garante può provvedere sulle spese del procedimento. Infine, ove sorgano difficoltà o contestazioni in ordine all'esecuzione possono essere disposte modalità di attuazione, sentite le parti. La statuizione sulle spese del procedimento

CamminoDiritto.it
ISSN 2532-9871

costituisce, ove non opposta, titolo esecutivo. (D.Lgs. n. 196 del 2003, art. 150). Dall'esame dei provvedimenti attribuiti alla competenza del Garante in sede di tutela "alternativa a quella giurisdizionale" così la sezione 3 del Titolo 1 (Tutela amministrativa e giurisdizionale), Capo 1, della Parte 3 (Tutela del'interessato e sanzioni) può escludersi che a tale Autorità sia attribuita la cognizione di domande risarcitorie, da ritenersi coperta da riserva esclusiva di giurisdizione ordinaria. La fondatezza di tale ultima affermazione, tuttavia, deve essere confrontata con il principio dell'alternatività delle tutele contenuto nel D.Lgs. n. 196 del 2003, art. 145, commi 2 e 3, secondo i quali:

a) il ricorso al Garante non può essere proposto se per il medesimo oggetto e tra le stesse parti è stata già adita l'autorità giudiziaria;

b) la presentazione del ricorso al Garante rende improponibile un'ulteriore domanda davanti all'autorità giudiziaria ordinaria tra le stesse parti e per lo stesso oggetto.

Come espressamente stabilito dalle disposizioni esaminate l'alternatività riguarda esclusivamente le domande aventi un identico oggetto, ovvero quelle che, se pendenti contestualmente davanti a più giudici, possono, in via generale, essere assoggettate al regime processuale della litispendenza o della continenza. Si tratta delle domande che richiedono interventi di natura preventiva, inibitoria o conformativa, potendo il Garante indicare modalità concrete di cessazione del trattamento illecito dei dati.

La domanda di risarcimento del danno patrimoniale o non patrimoniale ha causa petendi e petitum radicalmente divergenti da quelle sopra esaminate ed è destinata ad una declaratoria d'inammissibilità se proposta davanti al Garante. Peraltro, in numerose pronunce (ex multis 19/2/2002 doc. web. 1063674; 5 ottobre 2006 doc. web. 135919), il Garante ha ritenuto inammissibile il ricorso contenente una domanda risarcitoria, ritenendosi privo di competenza al riguardo.

L'accoglimento del ricorso, totale o parziale, da parte del Garante può, in conclusione, facilitare il ricorso alla tutela risarcitoria davanti all'autorità giudiziaria ordinaria, ma non escluderla.

Diversamente ragionando, dovrebbe ritenersi alternativamente che scelta la strada della tutela inibitoria (e preventiva), sia negata quella risarcitoria, oppure che, nonostante il riconoscimento del trattamento illecito dei dati personali, la parte sia tenuta ad un'impugnazione del provvedimento del Garante al solo fine di richiedere il risarcimento del danno e non incorrere nella sanzione di tardività dell'azione.

CamminoDiritto.it
ISSN 2532-9871

Quest'ultima soluzione è in netto contrasto con il canone costituzionale della ragionevolezza.

La prima introduce un impedimento all'ottenimento della tutela piena di un diritto fondamentale quale quello in gioco, del tutto incompatibile con l'art. 24 Cost.. Diversa è la soluzione in caso di rigetto del ricorso da parte del Garante. In tale ipotesi, condicio sine qua non per adire l'autorità giudiziaria è l'impugnazione tempestiva del provvedimento di diniego, con conseguente facoltà di proporre la connessa domanda risarcitoria unitamente a quella relativa all'accertamento della illiceità del trattamento dei dati.

Nella specie, contrariamente a quanto sostenuto nella sentenza impugnata, il provvedimento del Garante non è stato di rigetto integrale del ricorso proposto ma soltanto parziale.

Per la parte più consistente d'illecito trattamento di dati denunciata nel ricorso vi è stata l'adesione spontanea del titolare alla cancellazione ed eliminazione dei dati in oggetto. Esclusivamente rispetto ad essi i ricorrenti hanno legittimamente proposto domanda risarcitoria, senza contestare (non avendo alcun interesse al riguardo) la statuizione di non luogo a provvedere, in quanto logicamente conseguente alla predetta adesione".

Inoltre, indipendentemente dalla qualificazione come pericolosa delle attività di trattamento dei dati, la predisposizione di una regola speciale di responsabilità corrisponde all'individuazione di un criterio di imputazione più gravoso rispetto a quello previsto nell'art. 2043 c.c.: l'art. 15 D.Lgs. n. 196/03, che non intende qualificare come pericolose tutte, indistintamente, le attività di trattamento dei dati personali, non esprime una mera regola probatoria **ma una specifica regola d'imputazione che il legislatore ha consapevolmente introdotto**.

Il legislatore nazionale ha predisposto una tutela rafforzata, e tendenzialmente esaustiva, dei soggetti danneggiati dalle operazioni di trattamento dei dati, aggiungendo agli strumenti a carattere preventivo il tradizionale rimedio risarcitorio e rafforzando quest'ultimo mediante la predisposizione di un regime di responsabilità oggettiva.

6. Le misure efficaci per una reale protezione dei dati trattati.

Il Gruppo art. 29 rimarca il carattere potenzialmente pericoloso del trattamento dei dati personali, riconducendo l'"assoluta necessità" di predisporre "misure efficaci" per una "reale protezione" dei dati a molteplici ragioni: l'incessante progresso tecnologico ed il

CamminoDiritto.it
ISSN 2532-9871

correlato sviluppo dei sistemi di informazione e di comunicazione determinano la proliferazione dei dati personali raccolti, selezionati, trasferiti o conservati; l'aumento "quantitativo" dei dati e la sempre più diffusa capacità degli utenti di utilizzare le nuove tecnologie provocano un aumento anche "qualitativo" degli stessi e, dunque, il crescente "valore" dei dati, in termini economici, sociali e politici; i pregiudizi che la violazione della privacy può cagionare nei settori pubblico e privato sono potenzialmente "devastanti", in termini economici e di reputazione, soprattutto nell'ambito di settori "sensibili" quali il "governo elettronico" e la "sanità elettronica".

E' ragionevole, seguendo questa linea interpretativa, valorizzare plurimi indici sintomatici della "pericolosità", in astratto, delle operazioni di trattamento: la costante globalizzazione dell'economia e della società, la dimensione mondiale del trattamento dei dati, nonché la crescente complessità dei contesti nei quali i dati sono utilizzati, correlata alla sempre più diffusa differenziazione organizzativa nel settore pubblico e privato. La Direttiva 95/46/C.E., la fonte normativa più importante, nel diritto europeo, in materia di protezione dei dati dell'Unione, delineava il regime comunitario di responsabilità in plurime disposizioni.

L'art. 17, rubricato "sicurezza dei trattamenti", prevedeva l'obbligo di attuare "misure tecniche ed organizzative" idonee a garantire "la protezione dei dati personali dalla distruzione accidentale o illecita", dalla perdita accidentale o dall'alterazione, diffusione o accesso non autorizzati, specificando che "tali misure devono garantire (…) un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere".

In particolare, il paragrafo 2 dell'art. 23 esonerava da responsabilità il "titolare" del trattamento nel caso in cui l'evento dannoso non gli era imputabile. Il Regolamento europeo n. 2016/679, pur valorizzando, in numerose disposizioni, la rilevanza del grado di "rischio" delle operazioni effettuate, non contiene norme che definiscano espressamente come "pericolose" le operazioni di trattamento dei dati.

7. Conclusioni.

Escluso che il Regolamento abbia un carattere innovativo rispetto all'art. 15 del "Codice privacy" italiano (ovvero che imponga l'abrogazione, la modifica o una diversa interpretazione di tale norma), e mancando ancora una più analitica regolamentazione del regime comunitario di responsabilità civile per violazione delle norme di tutela dei dati personali, il richiamo testuale della normativa italiana all'art. 2050 c.c. resta efficace, non si riscontrano differenze significative sul piano applicativo e non si registrano elementi che giustifichino un'esegesi della norma diversa o innovativa rispetto alle elaborazioni

CamminoDiritto.it
ISSN 2532-9871

antecedenti il Regolamento. A tal fine si può sostenere che:

gli artt. 23 della Direttiva 95/46/CE e 82 del Regolamento 2016/679 esprimono la medesima previsione di esonero da responsabilità secondo la quale **il presunto danneggiante non è responsabile ove dimostri che l'evento dannoso non gli è imputabile**; né la Direttiva né il Regolamento contengono disposizioni che specifichino, in modo puntuale, in quali circostanze o a quali condizioni l'evento dannoso non è imputabile a colui che ha trattato il dato. Il legislatore comunitario non ha inteso disporre in modo più specifico rispetto al passato in merito al modello di responsabilità civile per illegittimo trattamento dei dati personali.

L'art. 82, rubricato "diritto al risarcimento e responsabilità", esonera da responsabilità il titolare o il responsabile del trattamento che dimostri che l'evento dannoso non gli è imputabile (art. 82, paragrafo 3), specificando che al "responsabile" del trattamento non è ascrivibile alcuna responsabilità se ha adempiuto agli specifici obblighi del Regolamento o ha agito in modo conforme alle legittime istruzioni del "titolare" del trattamento (art. 82, paragrafo 2).

Dunque, il par. 2 dell'art. 82 non contiene una previsione che avalli la tesi della valenza innovativa del Regolamento rispetto all'art. 15 della normativa italiana.

D'altro canto, non può ritenersi che il Regolamento europeo preveda un regime di attenuazione della responsabilità civile, posto che:

il "titolare" del trattamento è responsabile, oltre che per le violazioni del Regolamento, per le violazioni di "altre norme del diritto dell'Unione o degli Stati membri" ed anche per il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del Regolamento e alle disposizioni degli Stati membri di specificazione dello stesso Regolamento[56]; **il "responsabile"** del trattamento è sempre responsabile, in solido con il titolare, ove non adempia al dovere generale di avvisare il titolare del trattamento in caso di condotte non conformi[57]; il Regolamento europeo persegue i fini di "assicurare un livello coerente ed elevato di protezione delle persone fisiche"[58], garantire, in materia di protezione dei dati, "un quadro più solido e coerente" di quello garantito dalla Direttiva 95/46/CE[59], **elevare la protezione dei dati** in conformità alla rapidità dell'evoluzione tecnologica della "società digitale" implicante l'aumento, in modo significativo, **della condivisione e della raccolta dei dati personali**[60]. Dunque, il confronto, anche analitico, tra la Direttiva 95/46/CE, il Regolamento europeo ed il D.Lgs. n. 196/03 conferma che:

obiettivo comune del legislatore nazionale e di quello comunitario è la predisposizione di uno strumento di tutela risarcitoria idoneo a reprimere gli illeciti ed a tutelare

CamminoDiritto.it
ISSN 2532-9871

efficacemente i danneggiati, onerati della sola prova del danno e del nesso di causalità, gravando, invece, sui presunti responsabili la prova liberatoria; non appare ragionevole un'interpretazione dell'art. 82 non coerente con l'obiettivo di piena ed efficace tutela dell'interessato; tutte le discipline normative, nazionali e comunitarie, prevedono, in sostanza, l'inversione dell'onere della prova, dovendo ritenersi che il quid pluris dell'art. 15 della normativa italiana consista nell'individuazione del contenuto sostanziale della prova liberatoria.

Note e riferimenti bibliografici

[1] Con documentazione degli adempimenti privacy presi in carico, il controllo sui trattamenti effettuati, con responsabilità e compiti assegnati, con misure di sicurezza implementate. [2] Sia in fase di determinazione dei mezzi di trattamento che nel corso del trattamento, il titolare adotta adeguate misure tecniche/organizzative/procedurali, come ad esempio la pseudoanonimizzazione, per soddisfare principi e requisiti del G.D.P.R. [3] Come pre-impostazione, il titolare adotta adeguate misure tecniche/organizzative/procedurali, tali che, siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento, in termini di quantità dei dati personali raccolti, estensione del loro trattamento, periodo di conservazione e l'accessibilità. [4] Art. 25, Regolamento (UE) 2016/679. [5] "Per dato personale si intende qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". [6] "«dato personale»: 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" [7] "«trattamento»:qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione". [8] Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di

CamminoDiritto.it
ISSN 2532-9871

un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo. [9] Cfr. Cass. civ. sez. III, 20/05/2015, n. 10280. [10] Ora rientranti, a seguito del vigente G.D.P.R, nella nozione di "particolari categorie di dati". [11] Cfr. Cass. civ. sez. III, 20/05/2015, n. 10280. [12] Considerando 4, Regolamento UE 2016/679. [13] Artt. 7 e 13 D.Lgs. n. 196/03. [14] Art. 15 D.Lgs. n. 196/03: 1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali e' tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale e' risarcibile anche in caso di violazione dell'articolo 11. Art. 2050 c.c.: Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno. Art. 11 D.Lgs. n. 196/03: 1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalita' per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. 2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati. [15] Cfr. Cass. civ., sez. I, 25/01/2017, n. 1931. [16] Cfr. Cass., 23/05/2016, n. 10638; Cass., 10/03/2006, n. 5254. [17] La sentenza ritiene che sia orientamento maggioritario la ricostruzione in termini di colpa presunta della responsabilità di cui all'art. 2050. [18] Cfr. Cass. civ. sez. I, 19/05/2014 n. 10947; Cass. civ., sez. I, 13/05/2015 n. 9785. [19] Cfr., tra i più recenti: Linee-guida sui responsabili della protezione dei dati (RPD), adottate il 13/12/16 ed emendate il 5/04/17; Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, adottate il 4/04/17 ed emendate il 4/10/17; Linee-guida riguardanti l'applicazione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679, adottate il 3/10/2017 [20] Art. 24, Regolamento (UE) 2016/679: 1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono

CamminoDiritto.it
ISSN 2532-9871

l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento. Art. 28, Regolamento (UE) 2016/679: 1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. (…) 10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione. Art. 82, Regolamento (UE) 2016/679: 1. 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. 2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento. 3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile. 4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato. 5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2. 6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2. [21] Consistente nell'inosservanza delle condizioni di legittimità del trattamento. [22] Riservatezza, identità personale, dignità. [23] Cfr. Trib. Milano, 28/09/2016, n. 10374. [24] Diverso dal vero e proprio diritto all'oblio, cioè il diritto ad essere dimenticato. [25] Cfr. Trib. Milano, 28/09/2016, n. 10374. [26] Cfr. Trib. Roma, sez. I civ., 3/12/2015 n. 23771. [27] Cfr. Cass. civ. sez I , 24/06/2016, n. 13161. [28] Cfr. Cass. civ. sez I , 24/06/2016, n. 13161. [29] Cfr. Tribunale di Biella, sentenza 26-29 marzo 2003 n. 24. [30] Cfr. Cass. civ, sez. III, 25/11/2014, n. 24986. [31] Cfr. Trib. Bari, sez. II, 23/07/2010, n. 2637. [32] Cfr. Corte App. Campobasso, sentenza 34, sez. civile, del 17/02/2015. [33] Cfr.

CamminoDiritto.it
ISSN 2532-9871

Cass. ord. 23/05/2013, n. 12749. [34] Cfr. Cass. civ., sez. I, 1/04/2009, n. 7958. [35] Cfr. Cass. civ., sez. I, 25/01/2017, n. 1931. [36] Cfr. Cass. civ., sez. I, 25/01/2017, n. 1931, cit., conforme, Cass. 28/05/2012, n. 8451. [37] Cfr. Cass. civ., sez. un., 27/12/2017, n. 30981, applicando tale principio ad una banca, accolgono il ricorso di un correntista sul cui estratto conto veniva indicato il riferimento alla L. n. 210/92 che riconosce il diritto ad un assegno bimestrale per chi è stato contagiato da sangue infetto; anche in questo caso devono applicarsi le cautele relative al trattamento dei dati sensibili. [38] Cfr. Cass. civ. Sez. I, 13/02/2012, n. 2034. [39] Cfr. Cass. civ., sez. VI, 05/09/2014, n. 18812. [40] Cfr. Cass. civ., sez. II, 08/09/2011. [41] Cfr. Cass. civ., sez. II, 4/01/2011, n. 186. [42] Cfr. Cass. pen., sez. III, 28/03/2017, n. 15221. [43] Cfr. Trib. Siracusa, 15/03/12; Trib. Palermo, 12/01/10. [44] Cfr. Giud. Pace di Ottaviano, 30/09/11. [45] Cfr. Trib. Siracusa, 15/03/12. [46] Cfr. Giud. Pace di Milano, Sez. IV, 7 gennaio 2011, n. 41. [47] Cfr. Cass. civ. Sez. III, 11/02/2009, n. 3350. [48] Nella specie, relativa ad un caso di furto d'identità ed utilizzazione da parte del reo di un documento altrui in nulla alterato o modificato, al fine di aprire conti correnti ed emettere assegni, la Corte esclude che l'attività bancaria possa essere considerata attività pericolosa e, tuttavia, pone a carico della banca, e non del danneggiato, l'onere di fornire la prova della scusabilità del suo errore. [49] Cfr. Cass. civ., sez. I, 23/05/2016, n. 10638. [50] Cfr. Cass. civ., sez. I, 12/06/2007, n. 13777. [51] Cfr. Cassazione civile, sez. III, 15/07/2014, n. 16133. [52] Cfr. Cass., 18 luglio 2013, n. 17602. [53] Cfr. Cass. n. 17602 del 2013, cit.; Cass., 4 gennaio 2011, n. 186. [54] Cfr. Cassazione civile, sez. VI 05/09/2014 n. 18812. [55] Cfr. Cassazione civile, sez. I, 17/09/2014, n. 19534. [56] Considerando 146, Regolamento (UE) 2016/679. [57] Art. 28, paragrafo 3, Regolamento (UE) 2016/679. [58] Considerando 10, Regolamento (UE) 2016/679. [59] Considerandi 6 - 9, Regolamento (UE) 2016/679. [60] Considerando 6, Regolamento (UE) 2016/679.