A. Albanese - G. Andreotti - E. Arezzo - A. Astone - F. Astone
P. Bartolomucci - A. Bellelli - R. Bocchini - G. Capo - R. Carleo
R. Catalano - M. Cavaliere - G. Ciacci - V. Citarella - M. D'Ambrosio
G. D'Angelo - V. D'Antonio - E. De Chiara - A. Di Biase - F. Di Ciommo
A. Fachechi - V. Falce - L. Fernandez Del Moral Dominguez
E. Forgillo - L. Gatt - S. Giova - L. Guffanti Pesenti - F. Lazzarelli
B. Liberatore - E. Minervini - M. Montanari - S. Monticelli
R. Omodei Salè - T. Pasquino - A. Renda - M. Romano - L. Ruggeri
P. Sammarco - F. Sbordone - S. Sica - M. Tescaro - S. Troiano - F. Trubiani

MANUALE DI DIRITTO PRIVATO DELL'INFORMATICA

a cura di

Roberto Bocchini

Edizioni Scientifiche Italiane

Capitolo IV

La responsabilità per illecito trattamento di dati personali

Gianluigi Ciacci

1. Premessa: nozioni base sulla disciplina in materia di protezione dati personali

Dalla «privacy» alla «protezione dei dati personali»

Storicamente la nascita dell'attenzione per la protezione delle informazioni relative all'individuo si fa risalire alla fine dell'800 in U.S.A., precisamente al dicembre del 1890, quando venne pubblicato sull'Harvard Law Review il saggio «The Right to Privacy», scritto da Samuel D. Warren e Louis D. Brandeis. In tale opera gli autori affermavano che ognuno aveva il diritto di escludere gli altri dalla propria sfera privata (in cui facevano rientrare tutti quei valori dell'individuo che devono essere protetti da ingerenze esterne), un «diritto di essere lasciato solo» (*right to be let alone*), contrappeso e limite dell'antitetico diritto di informare ed essere informato, indicato appunto quale «diritto alla riservatezza».

Nei seguenti decenni il concetto venne sviluppato in stretto collegamento con il diritto di informazione e l'evolversi della tecnologia: in particolare quando l'avvento dei computer, e la loro esponenziale diffusione, iniziò a realizzare la nascita di una nuova forma di potere, il c.d. «potere informatico», rendendo sempre più sentita l'esigenza di proteggersi dalla crescente, e tecnologicamente evoluta, ingerenza nella propria intimità. Tale esigenza venne soddisfatta con due diverse modalità: da una parte, ampliando la portata del diritto alla riservatezza, non più «passivo», finalizzato ad escludere gli altri, ma inteso come un diritto «attivo», di controllare l'uso che viene fatto dei dati del soggetto interessato; dall'altra, emanando, a partire dagli anni settanta, una serie di normative specifiche volte a disciplinare la delicata realtà del diritto alla riservatezza nel contesto delle prime banche di dati personali.

Successivamente è ancora l'evoluzione tecnologica a far nuovamente mutare ambito e portata del diritto alla riservatezza, sia con il passaggio dall'informatica accentrata all'informatica distribuita, ed ancora di più quando nacque e si diffuse la Rete delle Reti, Internet, che, oltre a far diventare l'uso del computer veramente di massa, sollevò ulteriori e complicati problemi di protezione delle informazioni relative agli individui. Rendendo di conseguenza necessario giungere ad una tutela che prescindesse dalla «riservatezza», dalla «delicatezza», dalla «sensibilità» dei dati personali: e addirittura dalla stessa volontà di protezione della persona a cui l'infor-

 ISBN 978-88-495-5334-5

mazione si riferisce, o comunque dalla consapevolezza della sua necessità. A tale proposito le più recenti normative in materia non parlano più di «diritto alla riservatezza», di privacy, o almeno non solo, ma di «diritto alla protezione dei dati personali». Nuova impostazione che si concretizza con la pubblicazione della Direttiva 95/46/CE, e quindi con il suo recepimento nei vari Paesi membri: realizzata nel nostro dapprima con la legge 31 dicembre 1996 n. 675, e quindi con il d.lgs. 30 giugno 2003 n. 196, dettato per correggere e semplificare la precedente disciplina[1].

Normativa che è però risultata di non facile lettura e comprensione, ricca di obblighi spesso avvertiti da chi li doveva rispettare come inutili, e dunque percepita come ennesima espressione di una burocrazia vessatoria e impedimento allo sviluppo delle proprie attività[2]. Inoltre, essendo strettamente legata alla realtà del trattamento automatizzato delle informazioni, l'evoluzione della tecnologia, il passaggio all'Internet 2.0, e il conseguente mutamento sociale realizzato dall'uso massivo della Rete e dei suoi servizi, ha reso necessario un suo aggiornamento (si pensi che quando negli anni novanta vennero emanate le prime leggi con la nuova impostazione solo una minima parte della popolazione europea, intorno all'1%, usava Internet[3], e non esistevano *social network*, *tablet* e *app*).

Il Regolamento UE 2016/679

Per ovviare alla situazione appena descritta, che ha portato in pratica al fallimento del sistema di protezione della Direttiva del 1995, tra l'altro non più aggiornata alle innovative attività di trattamento dei dati degli ultimi anni, il Parlamento europeo il 27 aprile 2016 ha emanato il Regolamento 2016/679 sulla protezione dei dati personali[4] che, dal 25 maggio 2018, ha

[1] Volendo schematizzare quanto appena riportato circa l'evoluzione della disciplina in materia di protezione dei dati personali, possiamo identificare tre distinte fasi: la prima, quella che vede la nascita del «right to privacy», concepito come un diritto passivo, di escludere gli altri dalla propria sfera privata; la seconda, legata all'evoluzione tecnologica, quella della diffusione dei computer, e normativa, con le prime leggi dedicate alla disciplina delle banche di dati nominativi, periodo in cui il diritto alla riservatezza diventa attivo, con la nascita di una serie di facoltà in capo al soggetto i cui dati vengono utilizzati da altri; la terza, in cui l'ulteriore diffusione dell'informatica nella società, l'avvento della rete Internet, hanno fatto ritenere necessario aggiungere al *right to privacy*, sempre più in crisi, anche un nuovo diritto, quello alla protezione dei dati personali.

[2] Conseguenza di tale percezione è stata la forte carenza negli anni di una generalizzata «cultura» della tutela delle informazioni relative agli individui (ancora oggi si confonde il diritto alla riservatezza con quello alla protezione dei dati personali), la mancata consapevolezza dell'importanza delle proprie informazioni e della necessità della loro salvaguardia, la disattenzione politica al problema, lo scarso livello di adeguamento alla legge delle strutture dei vari titolari, privati ed anche pubblici.

[3] Oggi sono arrivati all'80%; in Italia all'epoca gli utenti erano intorno agli 80.000, oggi sono circa 50 milioni.

[4] 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 per-

ISBN 978-88-495-5334-5

sostituito, o comunque integrato, tutte le normative dei Paesi dell'Unione: tra queste anche il d.lgs. 196/2003 italiano, il c.d. Codice privacy, disciplina la cui applicazione ha, come detto, sollevato negli anni diverse difficoltà.

La genesi della normativa europea va ricercata, da una parte, nell'aumento esponenziale delle attività di raccolta e di condivisione dei dati, sia ad opera di soggetti pubblici che privati; nonché, dall'altra, nel repentino sviluppo delle nuove tecnologie che ha facilitato e moltiplicato le occasioni di circolazione delle informazioni relative agli individui, che oggi spesso pubblicano in prima persona, più o meno consapevolmente, i propri dati personali. Evoluzione che ha dunque reso necessario andare oltre la precedente disciplina, con una normativa che, in quanto Regolamento, è immediatamente applicabile in tutti i Paesi dell'Unione con il medesimo testo: normativa che ha introdotto un diverso approccio alla protezione dei dati personali nella società digitale, basato su nuovi strumenti che hanno permesso di trasformare il fallimento del sistema di tutela degli anni '90, avente fonte nella Direttiva 95/45/CEE, in un successo. Tra tali strumenti si possono ricordare l'ingente aumento dell'importo delle sanzioni per l'inadempimento dei vari obblighi, l'introduzione di un sistema basato sulla responsabilizzazione del titolare (c.d. *accountability*), e una serie di scelte «strategiche» nella costruzione della disciplina normativa (ad esempio, l'introduzione della figura e del ruolo del Responsabile per la Protezione dei Dati Personali, comunemente DPO, dell'obbligo di tenuta di un Registro dei trattamenti come momento di «autoconsapevolezza» del titolare, l'obbligo di denuncia dei c.d. *data breach*, …).

A parte gli indicati obblighi, introdotti proprio per realizzare un miglioramento del livello di protezione delle informazioni, il successo è stato reso possibile principalmente dalla natura «sostanzialista» del Regolamento 2016/679, il cui metodo di tutela non si risolve solo nel rispetto formale degli adempimenti richiesti, come in quello precedente, ma nella costruzione di un'effettiva, ed efficace, protezione delle informazioni personali degli individui: si è passati cioè da una logica «di adempimento» (il mero rispetto di obblighi precostituiti ed uguali per tutti, semplicemente rispettati dai titolari del trattamento, senza curarsi del risultato dell'adeguamento al loro disposto) a quella di sistema (dove prevale l'efficacia di questo, basato come detto sulla responsabilizzazione, sull'*accountability* dei titolari). Ancora, il cambiamento ha riguardato proprio l'oggetto della disciplina, la sua finalità: in particolare, prima, con la Direttiva 95/46/CE, si voleva assicurare la protezione dei dati personali e la loro libera circolazione; oggi, con il Regolamen-

sonali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) su Internet all'indirizzo ufficiale *http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679* citato frequentemente con l'acronimo GDPR (*General Data Protection Regulation*).

 ISBN 978-88-495-5334-5

to 2016/679, si inquadra invece la protezione dei dati personali quale diritto fondamentale e inviolabile della persona, e si ritiene prioritario rafforzare la fiducia degli interessati sulla tutela forte delle informazioni, stabilendo un quadro normativo adeguato allo sviluppo dell'economia digitale.

Cambiamento di impostazione che riporta centrale proprio l'importanza della tutela delle informazioni relative agli individui, come d'altro canto era già previsto in due fonti di primaria importanza per l'Europa: fonti che devono essere tenute presenti nell'analizzare, valutare e disciplinare le attività sulle informazioni relative agli individui, e quindi anche quelle collegate ai nuovi fenomeni tecnologici (su tutti l'intelligenza artificiale).

La prima è la Carta dei diritti fondamentali della UE, il cui art. 7 (intitolato «Rispetto della vita privata e della vita familiare») testualmente dispone «ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni»; mentre l'art. 8 (intitolato proprio «Protezione dei dati di carattere personale»), sancisce «1. ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano; 2. 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. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica; 3. il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

La seconda fonte è il c.d. Trattato sul funzionamento della UE, il cui art. 16 prevede al par. 1 che «Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano», e al par. 2 «Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti».

Ma tornando al Regolamento 2016/679, a livello definitorio, per l'argomento trattato nel presente capitolo, e senza dilungarsi negli ulteriori aspetti della complessa disciplina, occorre innanzitutto riportare cosa intenda per «trattamento», «dato personale», «titolare» e «responsabile», e dunque individuare quando si realizza la fattispecie di «trattamento illecito». Dal primo punto di vista, secondo l'art. 4 par. 1 n. 2 del Regolamento 2016/679, è 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

ISBN 978-88-495-5334-5

raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»: una definizione che, elencando sedici diversi tipi di operazioni che rientrano nel relativo concetto, porta a comprendere qualsiasi attività si possa fare con un'informazione personale. È poi il n. 1 del paragrafo 1 del medesimo art. 4 a specificare che «dato personale» è «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)»; mentre «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».

Prendendo poi in considerazione i soggetti collegati dal Regolamento alle attività di utilizzo di dati personali, rilevanti per il tema del presente capitolo, il «titolare del trattamento» è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»; mentre il «responsabile del trattamento» è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento» (art. 4 par. 1 nn. 7 e 8 del Regolamento); e infine «interessato» è la persona fisica a cui si riferiscono i dati.

2. Quando un trattamento di dati personali è illecito

Il trattamento illecito dei dati personali

Dal secondo punto di vista, a parte considerare «illecito» in generale il trattamento di dati personali che viene posto in essere dal titolare senza rispettare la disciplina in materia (e quindi ad esempio in mancanza dell'adeguamento della sua struttura al disposto del Regolamento europeo, e/o senza rispettare i particolari obblighi stabiliti per la determinata fattispecie di utilizzo delle informazioni relative agli individui), nello specifico deve ritenersi illecito il trattamento posto in essere in violazione dei principi generali stabiliti nel Regolamento 2016/679. Questi, previsti principalmente dai suoi artt. 5 e 25, devono essere considerati la base fondante della disciplina europea, rivestendo una particolare importanza per diversi motivi: come detto, innanzitutto perché sono le fondamenta sulle quali è stato costruito il sistema della protezione dei dati personali; poi perché da essi derivano i vari obblighi stabiliti dalla normativa (ad esempio, per la realizzazione del principio di trasparenza viene introdotto l'obbligo di dare l'informativa al soggetto interessato, oggetto degli artt. 13 e 14 del Regolamento); infine, dal lato applicativo, perché costituiscono il parametro necessario per interpretare correttamente il disposto del Regolamento, e quindi per capire, caso per caso, se l'attività che si vuole porre in essere possa essere o meno ritenuta legittima.

 ISBN 978-88-495-5334-5

Per determinare tale requisito, occorre partire dalla verifica del rispetto o meno del principio di liceità di cui all'art. 5, par. 1, lett. *a*), ed in particolare fare riferimento agli art. 6 e 9 del Regolamento, che stabiliscono le condizioni ricorrendo le quali esso viene raggiunto (la prima norma riferita all'uso delle informazioni «comuni», come nel caso di un indirizzo e-*mail*, mentre l'art. 9 a quello delle informazioni «particolari», come ad esempio un certificato medico)[5]: condizioni che consistono nelle c.d. «basi giuridiche del trattamento».

Queste rappresentano il fondamento giuridico dell'attività di trattamento, il motivo per cui il titolare utilizza le informazioni di uno o più determinati individui, e sono elencate dallo stesso Regolamento nelle norme appena indicate. Nella specie, il paragrafo 1 dell'art. 6 elenca i seguenti elementi di liceità per l'attività di trattamento di dati personali comuni (lettere *a-f*): il consenso dell'interessato; l'esecuzione di un contratto di cui l'interessato è parte, o di misure precontrattuali adottate su sua richiesta; l'adempimento di un obbligo di legge; la salvaguardia degli interessi vitali dell'interessato o di un'altra persona; l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; il perseguimento di un legittimo interesse del titolare o di terzi (a condizione che non prevalga il diritto alla tutela dell'interessato)[6].

Con riferimento poi alle basi giuridiche per legittimare l'attività di trattamento dei dati personali «particolari», la scelta del legislatore europeo nel redigere l'art. 9 è peculiare. Infatti, nel paragrafo 1 si parte da una netta affermazione: è vietato trattare tale categoria di informazioni personali, tranne riportare poi le eccezioni a questo divieto, che delineano le basi giuridiche che legittimano la relativa attività di trattamento su tali informazioni.

[5] Si ricorda che dati personali «comuni» (individuati in negativo, cioè non «particolari»), sono quelli che permettono l'identificazione, diretta o indiretta, di una persona fisica; invece, dati personali «particolari», che nella precedente disciplina venivano detti «sensibili», sono quelli esplicitamente previsti nell'art. 9, par. 1, e dunque quelli «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».

[6] Volendo riportare qualche esempio, il trattamento dei dati dei propri clienti posto in essere da un avvocato per l'assistenza in una procedura giudiziaria è *in esecuzione di un contratto* (nella specie, di patrocinio legale), e quindi ha come base giuridica l'art. 6, par. 1, lett. *b*); invece, il medico nell'emettere la propria fattura per la visita del suo paziente utilizza i relativi dati sulla base giuridica dell'*adempimento di un obbligo di legge* (art. 6, par. 1, lett. *c*); quando poi un'università utilizza le informazioni dei propri studenti sta *svolgendo un compito di interesse pubblico*, e può lecitamente farlo sulla base dell'art. 6, par. 1, lett. *e*); mentre il trattamento posto in essere tracciando gli spostamenti di interessati per contenere una pandemia, attraverso una particolare app del cellulare, ha come base giuridica la *salvaguardia degli interessi vitali* degli stessi (previsto dalla lett. *d* dell'art. 6).

ISBN 978-88-495-5334-5

Nella specie il paragrafo 2 (lettere *a-j*) ritiene utilizzabili i dati particolari ad esempio quando l'interessato ha espresso il proprio *consenso esplicito* al trattamento di tali dati personali per una o più finalità specifiche; il trattamento è necessario per *tutelare un interesse vitale dell'interessato* o di un altro individuo (qualora l'interessato si trovi nell'incapacità, fisica o giuridica, di prestare il proprio consenso); oppure quando riguarda *dati personali resi manifestamente pubblici* dall'interessato; o ancora nel caso di trattamento di dati relativi alla salute per finalità di cura, se il titolare opera in ambito sanitario[7].

Se dunque, come detto, vengono utilizzate una o più informazioni relative ad uno o più individui senza una delle basi giuridiche indicate negli artt. 6 e 9 del Regolamento (ad esempio il titolare non richiede il consenso dell'interessato nel caso voglia usare il suo indirizzo mail per inviargli offerte commerciali), il trattamento di quelle informazioni deve considerarsi illecito.

Dal punto di vista soggettivo, l'utilizzo delle informazioni in maniera contraria a quanto disposto dalla disciplina in materia di protezione dei dati personali può essere realizzato dal titolare del trattamento, ma l'inadempimento può essere posto in essere anche dal responsabile del trattamento, come detto il soggetto esterno alla struttura del titolare che utilizza i dati personali di questo in suo nome e per suo conto, fornendogli un determinato servizio (si pensi ad esempio al consulente del lavoro che predispone le buste paga dei dipendenti del titolare, suo cliente: le informazioni relative al lavoratore, che permettono di individuare la somma del suo stipendio, fornite dal titolare, verranno utilizzate al solo scopo dell'elaborazione, e quindi consegna al datore, appunto delle buste paga). Secondo l'art. 28 del Regolamento 2016/679, tra i due soggetti verrà stipulato un apposito «contratto di nomina», in cui verranno regolamentati i rapporti tra le due parti con riferimento alle modalità che il fornitore del servizio dovrà seguire per adempiere agli obblighi stabiliti dal titolare e dalla disciplina normativa. Nel caso tali obblighi non vengano adempiuti dal responsabile esterno, si realizzerà da parte di questo un duplice illecito: nei confronti del titolare, di natura contrattuale, mentre per il mancato rispetto degli obblighi stabiliti

[7] Le altre ipotesi previste dall'art. 9 del Regolamento 2016/679 sono: il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, in presenza comunque di adeguate garanzie per i diritti fondamentali e gli interessi dell'interessato; il trattamento è effettuato, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali; il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria (o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali); il trattamento è necessario per motivi di interesse pubblico rilevante; il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica; il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

 ISBN 978-88-495-5334-5

dal Regolamento 2016 si rientrerà in un illecito extracontrattuale. In tale seconda ipotesi, la fattispecie sarà identica a quella derivante dalla violazione della disciplina in materia posta in essere dal titolare[8].

3. Le conseguenze di un trattamento illecito di dati personali

Le tre responsabilità per il trattamento illecito

Una volta accertata l'esistenza di un trattamento illecito di dati personali, e quindi nel caso il titolare (o il responsabile) ponga in essere una violazione della normativa in materia di protezione dei dati personali le conseguenze in cui può incorrere, previste dal Regolamento 2016/679 e dal d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, sono di natura amministrativa, penale o civile. Con riferimento al primo tipo di responsabilità, quella *amministrativa*, rispetto alla disciplina precedente (in particolare indicata negli artt. 161-166 del d.lgs. 196/2003 originale) anche per questo settore si è avuto un vero e proprio cambio di sistema: non più impostato sul tipo di violazione posta in essere, sul singolo obbligo inadempiuto (informativa inesatta o incompleta, mancata notificazione, misure di sicurezza minime non presenti, …), a cui corrispondeva la specifica sanzione, determinata indicando un importo tra un minimo ed un massimo (ad esempio l'omessa informativa nel caso di trattamento di dati personali comuni, sanzione da tremila a diciottomila euro), eventualmente aumentabile fino al triplo a seconda delle condizioni economiche del titolare; ma oggi costruito individuando di due sole sanzioni che si applicano a due diversi gruppi di violazioni (a seconda dell'importanza del relativo obbligo), con l'eliminazione dell'importo minimo delle stesse, e l'indicazione solo di quello massimo.

La responsabilità amministrativa

A tale proposito, costruito un sistema di sanzioni amministrative in questo modo, chiaramente l'autorità Garante (o eventualmente il giudice ordinario adito, visto che il Garante sull'applicazione delle sanzioni amministrative non ha una competenza esclusiva) non può procedere in maniera totalmente discrezionale: ma, oltre a dover motivare la sua decisione, si atterrà ai parametri di commisurazione delle sanzioni stabiliti nell'art. 83, par. 2 del Regolamento 679. Secondo tale norma infatti «le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso (…)» e tenendo in «debito conto» gli elementi in esso indi-

[8] Anzi, nel caso in cui il responsabile *ex* art. 28 iniziasse ad utilizzare i dati personali ricevuti dal titolare al fine di poter fornire il servizio da lui richiesto (ad esempio l'elenco dei dipendenti del titolare allo scopo di poter elaborare le loro buste paga) in contrasto con le istruzioni ricevute nel contratto «di nomina» (magari perché inizia ad utilizzarli per attività di marketing dei suoi, o di altri, ulteriori prodotti o servizi), l'attività che andrà a porre in essere, illecita, il suo comportamento, sarebbe «da titolare» vero e proprio, ma utilizzando dati acquisiti illegittimamente.

ISBN 978-88-495-5334-5

viduati, tra cui riportiamo: la natura, gravità e durata della violazione; le categorie di dati personali interessate dalla violazione; il carattere doloso o colposo della stessa; le misure di sicurezza predisposte per evitare il danno; il grado di responsabilità del titolare o del responsabile del trattamento; il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; eventuali violazioni precedenti; l'adesione a Codici di condotta; eventuali fattori aggravanti/attenuanti applicabili alle circostanze del caso.

Valutati tutti questi parametri, il Garante (o il giudice) applicherà una delle due sanzioni previste nell'art. 83, paragrafi 4 e 5 del Regolamento, individuando l'importo preciso che il titolare dovrà pagare. In particolare, il titolare sarà tenuto al pagamento di una somma fino a 10.000.000 di euro (o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore), ad esempio quando la violazione riguarda gli obblighi in tema di consenso dei minori (art. 8 del regolamento 2016/679), protezione dei dati «*by design*» (art. 25), mancata notificazione di un *data breach* (art. 33), mancata adozione di misure di sicurezza adeguate (art. 32), omessa nomina del responsabile per la protezione dei dati personali (il c.d. DPO) quando obbligatorio (art. 37). Invece, la sanzione sarà fino a 20.000.000 di euro (o, sempre per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore), nel caso ad esempio di violazione dei principi generali del trattamento stabiliti nell'art. 5, dei diritti degli interessati individuati dagli artt. 13 e ss. (non ultimo anche rispetto alla procedura che ne permette un corretto esercizio stabilita nell'art. 12) di inosservanza delle disposizioni relative al trasferimento dei dati all'estero (chiaramente in Paesi extra Ue), in particolare quelle degli artt. 44-49.

Integra tale costrutto quanto stabilito dal d.lgs. 196/2003 vigente, quello modificato dal d.lgs. 101/2018, che prevede, sempre nell'ambito del sistema delle due sole sanzioni stabilito dal Regolamento, alcune ulteriori fattispecie di violazione: integrazione resa possibile dall'art. 84 della normativa europea, che lascia facoltà agli Stati membri di prevedere ulteriori sanzioni amministrative pecuniarie[9].

In alternativa o in aggiunta a quelle indicate, il Garante potrà comminare le altre sanzioni amministrative previste dall'art. 58, par. 2 del Regolamento 679.

[9] Ad esempio, il nuovo art. 166 del d.lgs. 196/2003 vigente prevede al suo comma 1 che l'inadempimento del disposto dell'articolo 2-*quinquies*, comma 2, della stessa normativa, relativo all'informativa da rendere con linguaggio semplificato rilasciata ai minori di quattordici anni in occasione dell'offerta diretta di servizi della società dell'informazione, venga punito con la prima sanzione, quella dei 10 milioni di euro; mentre il comma 2 dell'art. 166 stabilisce la comminazione della sanzione più alta, quella dei 20 milioni di euro, per la violazione dell'art. 2-*quinquies*, comma 1, relativo alla raccolta del consenso prestato dai minori di quattordici anni sempre nella medesima fattispecie dell'offerta diretta di servizi della società dell'informazione.

 ISBN 978-88-495-5334-5

Ad esempio, in caso di violazione minore o se la sanzione pecuniaria costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto al trasgressore un «ammonimento» (così il *considerando* 148 del Regolamento).

La responsabilità penale

Per quanto riguarda poi la *responsabilità penale*, la disciplina europea non stabilisce norme in cui si prevedono le conseguenze delle violazioni di tipo penalistico, e dunque dispone che sarà facoltà per gli Stati membri introdurre disposizioni relative a sanzioni penali (*considerando* 149). Così, per l'Italia la fonte di tale tipo di responsabilità si trova principalmente nel d.lgs. 196/2003, come modificato dal d.lgs. 101/2018, che nel capo 2 del suo titolo III (artt. 167-172) disciplina le seguenti fattispecie: trattamento illecito di dati personali (art. 167), che a seconda delle ipotesi, viene sanzionato con la reclusione da 6 a 12 mesi se i dati trattati sono comuni, oppure da 1 a 3 anni, se il trattamento riguarda i dati di cui agli articoli 9 e 10 del Regolamento, o il trasferimento all'estero dei dati; comunicazione e diffusione illecita di dati su larga scala, ovvero di un archivio automatizzato o di una gran parte di esso (art. 167-*bis*), comportamento punito con la reclusione da 1 a 6 anni; falsità nelle dichiarazioni e notificazioni al Garante per la protezione dei dati personali (art. 168), sanzionata con la reclusione da 6 mesi a 3 anni, e inosservanza dei suoi provvedimenti dell'Autorità Garante (art. 170), comportamento che prevede la reclusione da 3 mesi a due anni.

La responsabilità civile

Infine, nell'ipotesi in cui l'illegittimo trattamento dei dati personali da parte del titolare porti alla realizzazione di un danno per l'interessato, è prevista la sua *responsabilità civile*, stabilita oggi dall'art. 82 del Regolamento 2016/679, e quindi dovrà procedere al risarcimento di tale danno: fattispecie che verrà approfondita nei prossimi paragrafi, sia con riferimento alla legislazione che ne ha regolamentato gli aspetti, sia rispetto alla produzione giurisprudenziale che ne ha interpretato il disposto; per poi concludere con una valutazione dell'attuale disciplina anche dal punto di vista della sua capacità di proteggere i dati personali rispetto al ristoro dell'interessato danneggiato dal trattamento illegittimo dei propri dati.

4. La disciplina normativa in materia di responsabilità civile per illecito trattamento di dati personali

Nell'analizzare come il Legislatore (europeo ed interno) ha regolamentato la fattispecie della responsabilità civile per illecito trattamento di dati personali in esame nel presente capitolo, occorre prendere le mosse da quanto disposto dalla c.d. «Direttiva madre», la 95/45/CEE, per poi verificare le norme poste a suo recepimento dalla disciplina del nostro Paese, e dunque prima quelle previste dalla l. 31 dicembre 1996 n. 675, e poi quelle del d.lgs. 30 giugno 2003 n. 196; infine, ci si soffermerà sulla disciplina in vigore, e quindi su quanto disposto dal Regolamento 2016/679.

ISBN 978-88-495-5334-5

La responsabilità civile precedente al Regolamento 2016/679

Nella Direttiva europea, la norma che prendeva in considerazione la fattispecie in esame era l'art. 23 (intitolata «Responsabilità»), il cui paragrafo 1 sanciva che gli Stati membri, nel recepire la fonte comunitaria nel loro ordinamento interno, «dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento», mentre secondo il paragrafo 2 il responsabile del trattamento «può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile»[10].

A parte notare che il termine utilizzato per il soggetto che «determina le finalità e gli strumenti del trattamento dei dati personali» «responsabile», mentre nella normativa italiana (sia nella prima fonte di recepimento, la l. 675/1996, che in quella successiva, il d.lgs. 196/2003), è chiamato «titolare», la disposizione riporta due affermazioni in linea di massima generiche e di principio, che confermano la disciplina civilistica della responsabilità extracontrattuale: in particolare, secondo il testo del paragrafo 2, di tipo oggettivo.

Risulta invece più rilevante la normativa interna di recepimento della Direttiva: il Legislatore del nostro Paese ha infatti specificato quanto affermato dal suo art. 23 citato, costruendo una disciplina volta a rendere effettiva la protezione dei dati personali anche dal punto di vista del rapporto giuridico tra chi svolge il trattamento dei dati personali e il soggetto a cui questi si riferiscono.

Così, secondo gli artt. 18 e 29 comma 9 della l. 31 dicembre 1996 n. 675, «Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile» e «il danno non patrimoniale è risarcibile anche nei casi di violazione dell'articolo 9»; ed esattamente nello stesso senso si poneva anche il d.lgs. 30 giugno 2003 n. 196, il c.d. Codice privacy, che regolamentava la responsabilità civile da trattamento illegittimo nel suo art. 15 (unendo dunque, in maniera maggiormente razionale, le due norme della l. 675 in un'unica disposizione), che al comma 1 sanciva «Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile», mentre al comma 2 prevedeva che «il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11».

La responsabilità civile da trattamento illecito e l'art. 2050 c.c.

In entrambi i casi il Legislatore qualificava dunque la responsabilità derivante dal trattamento illegittimo dei dati personali un'«attività pericolosa», richiamando espressamente il disposto dell'art. 2050 del codice civile,

[10] Secondo il *considerando* 55 della Direttiva, questo può avvenire «(…) segnatamente quando dimostra l'esistenza di un errore della persona interessata o un caso di forza maggiore».

 ISBN 978-88-495-5334-5

da cui deriva quindi un'ipotesi di responsabilità oggettiva; e in entrambi i casi, nel prevedere la possibilità di estendere il risarcimento anche al danno non patrimoniale, veniva fatto riferimento alla norma che enunciava le modalità in cui si deve svolgere l'utilizzo corretto delle informazioni relative agli individui (nella specie l'art. 9 della l. 675 e l'art. 11 del Codice privacy), e quindi ai c.d. «principi generali del trattamento»[11]. Il loro mancato rispetto portava cioè alla risarcibilità di tale tipologia di danno.

Come è noto, la disciplina della responsabilità oggettiva implica che si prescinda, nella valutazione della responsabilità dell'autore del comportamento lesivo, da qualsiasi giudizio relativo alla presenza dell'elemento soggettivo (e quindi dall'esame della sussistenza o meno del dolo o della colpa[12]), ed allo stesso tempo comporti l'inversione legale dell'onere della prova[13]: basterà quindi il solo realizzarsi del danno in nesso causale con la condotta posta in essere dal titolare del trattamento affinché si concretizzi l'obbligo risarcitorio di questo, che dovrà direttamente provare di non essere responsabile. E, a tale proposito, si tenga presente che si rientra in un'ipotesi di responsabilità aggravata[14], che può essere evitata solo dimostrando di avere adottato «tutte le misure idonee ad evitare il danno»; ma, in tema di misure preventive (quindi, ad esempio, nel caso dell'adozione di misure di sicurezza per proteggere a livello tecnico i dati personali oggetto del trattamento da parte del titolare), se queste fossero state idonee il danno non si sarebbe verificato: il risarcimento sembrerebbe quindi evitabile, nell'ipotesi indicata, solo nel caso si riesca a provare il caso fortuito o la forza maggiore.

[11] Come detto, questi sono la base fondante della disciplina della protezione dei dati personali, i criteri che deve seguire il titolare quanto utilizza le informazioni relative agli individui: tra essi, ad esempio, il principio di pertinenza e non eccedenza, il principio di liceità e correttezza, il principio di qualità dei dati, il principio di finalità del trattamento.

[12] Il soggetto che ha causato il danno è quindi responsabile semplicemente perché ha posto in essere il relativo comportamento, a nulla rilevando se lo abbia fatto volutamente, o per mancata attenzione: anzi, se il danno si è realizzato, dovrà risarcirlo anche se ha prestato la massima attenzione perché ciò non avvenisse (caso tipico è quello del trasporto di sostanze pericolose, come quelle esplosive o tossiche).

[13] Normalmente nel nostro sistema processuale civile chi agisce in giudizio per far valere un proprio diritto deve dimostrare il fondamento della sua pretesa: se non ci riesce la sua domanda verrà rigettata e la causa persa. Nel caso di responsabilità civile c.d. aggravata (è questa l'ipotesi dell'esercizio di attività pericolose e dell'art. 15 del d.lgs. 196) il sistema della prova è invertito: è infatti il soggetto che ha causato il danno, e che viene chiamato in giudizio, a dover dimostrare la sua non responsabilità (non a caso, nella tradizione giuridica, si parla a tale proposito di «*probatio diabolica*»).

[14] A tale proposito, la Corte di Cassazione fornisce un'interpretazione ampia della fattispecie, includendo nella nozione di attività pericolosa anche tutte quelle attività atipiche «che, per la loro stessa natura o per le caratteristiche dei mezzi adoperati, comportino una rilevante possibilità di verificarsi di un danno (…) tenendo presente che anche un'attività per natura non pericolosa può diventarlo in ragione delle modalità con cui viene esercitata o dei mezzi impiegati per espletarla» (Cass. Civ., sez. III, 19 luglio 2018 n. 19180).

ISBN 978-88-495-5334-5

L'impostazione del sistema di responsabilità civile così delineato ha però sollevato diverse difficoltà applicative, in particolare quando si è dovuto coordinare la disciplina specifica della protezione dei dati personali con quella prettamente civilistica, in particolare anche in seguito agli interventi della giurisprudenza, come si vedrà nel successivo par. 5; ma altrettante difficoltà si sono poste a livello concettuale, anche se essenzialmente teorico, e quindi con minore ricaduta pratica.

Dal primo punto di vista, il problema ha riguardato nella specie la qualificazione del danno e la possibilità effettiva di un suo risarcimento; dal secondo punto di vista autorevole dottrina ha sollevato una forte critica circa l'inquadramento del trattamento «automatizzato» di dati personali quale «attività pericolosa» in sé[15].

In particolare veniva rilevato che tale impostazione evidenziava la prassi tipica del Legislatore del nostro Paese che più volte aveva considerato, probabilmente a causa di una poco chiara percezione e conoscenza delle nuove tecnologie, l'uso dell'informatica come attività ad alta potenzialità lesiva: concezione ereditata dai primi approcci normativi nel settore, ma comunque durante la fase iniziale di sviluppo dell'elaboratore elettronico, quello caratterizzato dai grandi computer, appannaggio di poche rilevanti strutture, e certamente non più adeguata alla realtà della c.d. «informatica distribuita», quella dei *personal computer*, già negli anni novanta ad uso sempre più comune nella collettività.

In realtà l'inquadramento della responsabilità da trattamento illecito dei dati personali nell'alveo dell'esercizio di attività pericolosa non deve essere collegato all'informatica in sé, all'uso del computer, ma all'attività di trattamento dei dati personali: come visto, da più fonti ritenuto un diritto fondamentale della persona, da tutelare in maniera piena ed efficace, anche attraverso l'applicazione di una responsabilità «da esercizio di attività pericolosa». Interpretazione che dunque permetterebbe di considerare il disposto della l. 675/1996 prima, e del d.lgs. 196/2003 dopo (sempre con riferimento alla sua versione originale), non un'espressione di un neoluddismo normativo, ma all'opposto la valorizzazione del dato personale e l'evidenziazione dell'importanza della sua tutela.

L'art. 82 del Regolamento 2016/679

Le conseguenze di natura civilistica del trattamento illecito di dati personali vengono disciplinate nel Regolamento 2016/679 dall'art. 82, il cui

[15] Secondo il Borruso infatti il riferimento all'art. 2050 cod. civ. è il frutto di una «pulsione emotiva fobica nei confronti dell'uso del computer che solo un retrogrado misoneismo può giustificare, e con ciò, tentare di arrestare il progresso in tutti i suoi aspetti che non permetterebbe di considerare serenamente la realtà, la quale denoterebbe che l'eventuale pericolo non risiede nell'uso del computer» (si veda R. Borruso e G. Ciacci, *Diritto Civile ed Informatica*, in *Trattato di Diritto Civile del Consiglio Nazionale del Notariato*, diretto da P. Perlingieri, Napoli, 2004, p. 173).

 ISBN 978-88-495-5334-5

par. 1 dispone che «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»; mentre il suo paragrafo 3 sancisce che «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»; gli altri paragrafi dell'articolo si occupano poi della responsabilità dal punto di vista dei soggetti che pongono in essere il trattamento, e quindi dal titolare e dal responsabile *ex* art. 28 (par. 2, 4, 5)[16]. Sulla base di tale norma, che riprende essenzialmente il testo della Direttiva 95/45/CEE, il risarcimento potrà essere quindi chiesto da «chiunque», non solo dall'interessato, e può riguardare i danni materiali e quelli immateriali; si conferma poi l'inquadramento della fattispecie nell'esercizio di attività pericolosa, e dunque per liberarsi dalla responsabilità risarcitoria il titolare, o eventualmente il responsabile esterno del trattamento, deve provare che l'evento dannoso non sia in alcun modo a lui imputabile (mentre l'interessato dovrà dimostrare l'esistenza del danno, la sussistenza di una condotta in violazione della normativa a tutela dei dati personali, e la relazione causale tra i primi due elementi, senza preoccuparsi dunque dell'elemento soggettivo dello stesso)[17].

Dal punto di vista della legittimazione passiva, come appena visto, la norma prende in considerazione oltre al titolare anche la figura del responsabile del trattamento *ex* art. 28: nel caso infatti di comportamento posto in essere da entrambi i soggetti «attivi» nell'utilizzo dei dati, coinvolti nel medesimo processo di trattamento, e il secondo non abbia rispettato il disposto del Regolamento europeo, o comunque le istruzioni impartitegli dal titolare nell'atto di nomina (così l'art. 82 par. 2), nell'eventualità vengano condannati al risarcimento saranno obbligati in solido (par. 4); e se uno dei due soggetti pagherà l'intero ammontare della sanzione, potrà poi rivalersi

[16] Rimane poi il par. 6, che disciplina la fattispecie dal punto di vista processuale, affermando che le azioni legali per ottenere il risarcimento sono presentate dinanzi alle autorità giurisdizionali competenti dello Stato membro (a norma del suo diritto interno), in particolare quello in cui il titolare o il responsabile abbiano uno stabilimento; in alternativa, si prende anche in considerazione quello in cui l'interessato risieda abitualmente (così l'art. 79 del Regolamento).

[17] Più precisamente, non solo viene confermata l'impostazione della disciplina precedente (come visto, trattamento dei dati quale esercizio di attività pericolosa, le cui conseguenze sono stabilite dall'art. 2050 c.c.), ma se ne estende la portata, in particolare dal punto di vista delle modalità con cui il titolare del trattamento possa esimersi dal risarcimento del danno. Infatti la dizione usata dall'articolo del codice prevede la prova liberatoria di «avere adottato tutte le misure idonee a evitare il danno», mentre l'art. 82, par. 3, del Regolamento richiede che l'evento dannoso non gli sia «in alcun modo imputabile»: rendendo così ancora più gravosa e difficile la prova liberatoria.

ISBN 978-88-495-5334-5

nei confronti dell'altro della parte di risarcimento corrispondente alla sua effettiva responsabilità (par. 5).

La disciplina delle conseguenze civilistiche del trattamento illecito dei dati personali stabilita nel Regolamento conferma quindi, pur se con una formulazione diversa, quanto era già stato disposto nel precedente sistema dettato in applicazione della Direttiva 95/46/CEE.

Occorre ora analizzare come la giurisprudenza del nostro Paese abbia poi interpretato tale disciplina (al momento essenzialmente quella del d.lgs. 196/20003 originario), sollevando una serie di problemi applicativi quando si è confrontata la specifica realtà della protezione dei dati personali con le categorie giuridiche «tradizionali» che caratterizzano la responsabilità civile extracontrattuale.

5. La giurisprudenza in materia di responsabilità civile per illecito trattamento di dati personali e di danno ingiusto

La giurisprudenza in materia

Con riferimento alla giurisprudenza che si è pronunciata sulla fattispecie in esame nel presente capitolo, le principali problematiche affrontate hanno riguardato il tema generale della responsabilità da esercizio di attività pericolosa, e poi nello specifico i presupposti e le condizioni per ottenere il risarcimento dei danni non patrimoniali conseguenti alla lesione del diritto alla protezione dei dati personali. Dal primo punto di vista, viene specificato che per poter qualificare un'attività come «pericolosa» debba essere considerato il contenuto intrinseco dell'attività stessa, mentre è superfluo verificare l'esistenza o meno di norme di legge che la definiscono in questo modo (Cassazione sezione III civile, sentenza 24 luglio 2012, n. 12900); e che, distinguendosi tra pericolosità della condotta e pericolosità dell'attività in quanto tale, è quest'ultima ad assumere rilievo, poiché riguarda un'attività che è potenzialmente dannosa di per sé a causa dell'alta percentuale delle conseguenze dannose che può provocare, in ragione della sua natura o della tipologia dei mezzi adoperati[18].

Rispetto poi alle conseguenze dell'inquadramento della responsabilità disciplinata dall'art. 2050 quale responsabilità oggettiva, ferma restando l'inversione dell'onere della prova e dunque la possibilità per il danneggiato di esimersi dal dimostrare l'elemento soggettivo della responsabilità, la

[18] Mentre la pericolosità della condotta riguarda un'attività normalmente innocua, che assume i caratteri della rischiosità a causa della condotta imprudente o negligente dell'operatore: in questo caso la condotta diventa elemento costitutivo della responsabilità ai sensi dell'art. 2043 c.c.; nell'ipotesi della pericolosità dell'attività è invece una componente proprio di quella disciplinata dall'art. 2050 c.c. (così Cassazione civile Sez. III sentenza del 21 ottobre 2005 n. 20357).

 ISBN 978-88-495-5334-5

Suprema Corte ha sancito il principio secondo il quale per poter rilevare il nesso di causalità tra, da una parte, un antecedente (cioè in questo caso l'esercizio dell'attività pericolosa) e, dall'altra, l'evento lesivo, debba ricorrere una duplice condizione: che si tratti di un antecedente necessario dell'evento e che non sia neutralizzato dalla sopravvenienza di un fatto di per sé idoneo a determinarlo (c.d. principio del nesso di causalità adeguata)[19].

Protezione dei dati personali e danno

Ma è il secondo punto di vista, che riguarda l'individuazione delle condizioni per ottenere il risarcimento dei danni non patrimoniali conseguenti alla lesione del diritto alla protezione dei dati personali, quello che suscita maggiori problemi nell'incontro tra le due diverse discipline. Infatti secondo la Corte di Cassazione, chiamata a pronunciarsi proprio circa la previsione dell'art. 15 del d.lgs. 196/2003, anche in questa specifica fattispecie il diritto al risarcimento del danno non patrimoniale deve essere bilanciato con la regola di tolleranza della lesione minima, quale corollario del principio di solidarietà ai sensi dell'art. 2 Costituzione. Conseguenza di ciò è che il danno non patrimoniale risarcibile a causa del trattamento illecito dei dati personali, pur se determinato da una lesione del diritto fondamentale alla loro protezione 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" (quale perdita di natura personale effettivamente patita dall'interessato) in quanto anche per tale diritto opera il bilanciamento con il principio di solidarietà *ex* art. 2 Cost., di cui il principio di tolleranza della lesione minima è intrinseco precipitato». In sintesi, nella fattispecie di cui all'art. 2050 c.c. (anche in caso venga applicato in conseguenza di un trattamento illecito di dati) il danno non può essere considerato «*in re ipsa*», cioè ritenuto esistente per il fatto stesso dello svolgimento dell'attività pericolosa: in caso contrario, la funzione stessa del risarcimento cambierebbe, passando da strumento di compensazione in una specie di «pena privata» per un comportamento lesivo; nell'eventuale giudizio dovrà quindi tenersi conto della suddetta regola di tolleranza, che così esclude dalle ipotesi risarcitorie tutte quelle in cui il danno non patrimoniale lamentato si riveli essere un mero fastidio o un lieve disagio[20].

Alla luce di tale orientamento della Cassazione, che si può ritenere consolidato, il problema di coordinamento tra le diverse discipline sorge allora

[19] Così rispettivamente Cassazione sentenze 15 febbraio 2003 n. 2312 e 4 maggio 2004 n. 8457.

[20] Numerose le pronunce della Suprema Corte in tal senso, sia con riferimento a fattispecie generali non coinvolte nella disciplina della protezione dei dati personali, sia specifiche al tema del presente capitolo: tra le altre si vedano Cass. Sez. Un., 11 novembre 2008, n. 26972; sezione VI Civile, ordinanza 11 gennaio 2016, n. 222; Sez. I, Sent. 25 gennaio 2017, n. 1931; Sez. 6 - 1, Ordinanza del 20 agosto 2020 n. 17383; Sez. I, ordinanza 26 febbraio - 26 aprile 2021, n. 11020.

ISBN 978-88-495-5334-5

per il contrasto tra l'interpretazione esposta (che porta all'applicazione della regola della tolleranza anche nella realtà dell'utilizzo delle informazioni relative agli individui nella società digitale) con la natura stessa del diritto alla protezione dei dati personali, riconosciuto, come si è detto, da due fonti di primaria importanza per l'Europa (la Carta dei diritti fondamentali della UE e il Trattato sul funzionamento della UE), e, seppure indirettamente, dalla stessa Costituzione italiana: fonti che devono essere tenute presenti nell'analizzare, valutare e disciplinare le attività sulle informazioni relative agli individui, e questo anche da parte delle Autorità (come in questo caso quelle giudiziarie) coinvolte nell'applicazione della normativa sulla protezione dei dati personali.

In particolare, secondo una parte della dottrina, i diritti inviolabili dell'individuo, in quanto tali, dovrebbero essere sempre risarciti in caso di trattamento illecito dei suoi dati, e quindi di loro lesione; e la valutazione da parte del giudice sull'intensità del pregiudizio alla luce del principio di tolleranza dovrebbe riguardare solo la quantificazione del danno, diventandone uno dei parametri da utilizzare, e non la sua esistenza. E si deve dunque ritenere non corretto che la previsione normativa circa l'ingiustizia della lesione dei diritti fondamentali da essi tutelati possa essere messa in discussione dalla valutazione dell'intensità del pregiudizio[21]: questo in particolare nell'ambito della complessa disciplina della protezione dei dati personali, che si caratterizza per l'amplissimo numero dei soggetti coinvolti, la peculiare realtà della società dell'informazione digitale nell'ambito della quale deve applicarsi, le specifiche tecnologiche che la permeano in costante evoluzione, tra l'altro oramai in maniera assolutamente imprevedibile e di difficile regolamentazione (si pensi alle applicazioni sempre più diffuse dell'Intelligenza Artificiale, con una rilevante potenzialità lesiva dei dati personali da esse utilizzate, e più in generale dei diritti individuali di tutti coloro che ne sono coinvolti)[22].

Disciplina rispetto alla quale, da ultimo, si deve anche tenere presente che lo stesso sistema della responsabilità civile costruito dal Regolamento 2016/679, quello dell'art. 82[23], è certamente volto ad una tutela più effi-

[21] «L'immissione nei diritti inviolabili della persona, come la sua riservatezza, comporta una intollerabilità intrinseca, che deve garantire l'*an* del risarcimento del danno alla persona e che non può essere letto in maniera diversa perché ciò porterebbe al paradosso che un diritto della persona, che è inviolabile di per sé, è però censurabile solo oltre una soglia minima quale l'accettabilità secondo i principi di solidarietà sociale».

[22] Tutti aspetti che renderebbero estremamente complessa, se non impossibile, la valutazione dell'intensità del pregiudizio (si veda a tale proposito, oltre nel testo, il par. 6).

[23] Che tra l'altro, come detto, con la dizione utilizzata nel suo paragrafo 3 per determinare cosa debba dimostrare il titolare del trattamento per evitare la condanna a risarcire il danno subito dall'interessato («che l'evento dannoso non gli è in alcun modo imputabile»), rispetto alla formulazione dell'art. 2050 del codice civile (dove gli viene chiesto «di avere

 ISBN 978-88-495-5334-5

cace dei dati degli interessati, che «dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito», come indicato nel *considerando* 146 del Regolamento UE. Norma che contribuisce anche all'indicato dibattito sulle condizioni per ottenere il risarcimento del danno in seguito al trattamento illegittimo dei dati personali: questo in particolare riportando che «il concetto di danno dovrebbe essere interpretato in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento» (la tutela degli interessati e dei loro dati personali), disposto difficilmente conciliabile con l'applicabilità della regola della tolleranza a tale fattispecie.

La sentenza CGUE del 4 maggio 2023

Si pone in questa prospettiva una recente sentenza della Corte di Giustizia UE (4 maggio 2023, causa C-300/21)[24], che ribadisce innanzitutto la necessità, per applicare l'art. 82 del Regolamento 2016/679, che si rispettino tre condizioni cumulative: il mancato rispetto del disposto della disciplina europea (considerato in generale, non limitato dunque solo ad alcune sue disposizioni, come ad esempio quelle relative ai principi generali del trattamento), un danno materiale o immateriale derivante da tale violazione e un nesso di causalità tra il danno e la violazione. Quindi secondo i giudici non basta il semplice inadempimento di un qualsiasi obbligo, come nel caso della responsabilità amministrativa o penale (che tra l'altro potrebbe addirittura prescindere da un nocumento nei confronti degli interessati e che, a tal riprova, può essere sanzionata dalle Autorità per la protezione dei dati personali degli Stati membri in modo indipendente da un danno), ma è necessaria la presenza di tutte e tre le condizioni. Il provvedimento diventa poi di estremo interesse per il tema oggetto del presente capitolo grazie al secondo punto del suo disposto, in cui la CGUE stabilisce il modo in cui debba essere interpretato l'art. 82 par. 1 del Regolamento[25].

La Corte nella specie evidenzia che il diritto al risarcimento non è riservato ai danni immateriali che raggiungono una determinata soglia di gravità. Il Regolamento 2016/679 non menziona infatti un requisito del genere, e comunque una tale restrizione alla possibilità di risarcimento sarebbe in contraddizione con l'ampia concezione delle nozioni di «danno» o di «pregiudizio» adottata dal legislatore europeo.

Tra l'altro, secondo la CGUE, subordinare il risarcimento di un danno

adottato tutte le misure idonee a evitare il danno»), dimostra una maggiore rigidità a vantaggio della tutela del soggetto i cui dati sono stati trattati in maniera illecita.

[24] Decisione rinvenibile direttamente nel sito web della Corte di Giustizia U.E., su Internet all'indirizzo *https://curia.europa.eu/juris/document/document.jsf;jsessionid=B74E09E07ECC12B0D524A783C0E3F673?text=&docid=273284&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1&cid=4335267* consultato il 12 giugno 2023

[25] «L'art. 82, par. 1 deve essere interpretato nel senso che: esso osta a una norma o una prassi nazionale che subordina il risarcimento di un danno immateriale, ai sensi di tale disposizione, alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità».

ISBN 978-88-495-5334-5

immateriale ad una determinata soglia di gravità, di discrezionale interpretazione da parte della giurisprudenza di ogni singolo Paese membro, rischierebbe di nuocere alla coerenza del regime istituito dal Regolamento (tipo di fonte scelta proprio per rendere la disciplina uguale in tutta l'Unione): e comunque di creare anomalie come quella del c.d. «*forum shopping*» da parte di un interessato particolarmente attento alla diversa sensibilità sull'argomento delle varie magistrature dei diversi Paesi europei (perché la graduazione da cui dipenderebbe la possibilità o meno di ottenere il risarcimento potrebbe infatti variare in funzione della valutazione dei giudici aditi)[26].

Il provvedimento della Corte di Giustizia del 4 maggio 2023 rende dunque, inequivocabilmente, l'indicata interpretazione della Cassazione sul sistema risarcitorio della normativa in materia di protezione dei dati personali non più corretta, e addirittura in contrasto con il disposto dell'art. 82 del Regolamento 2016/679: motivo per cui oggi risulta necessario una nuova riflessione sulle modalità di attuazione della disciplina in materia, che tenga comunque conto del peculiare contesto in cui dovrà essere applicata, e che si ponga dunque da un diverso punto di vista, maggiormente legato proprio al diritto dell'informatica.

6. Una lettura dell'attuale disciplina alla luce del diritto dell'informatica

La necessità di una riflessione alla luce del diritto dell'informatica

Dopo aver descritto la disciplina normativa sulla responsabilità civile per trattamento illecito dei dati personali, ed aver esaminato la giurisprudenza in materia, nel redigere le conclusioni del presente capitolo si deve completare l'analisi della responsabilità civile da trattamento illecito dei dati personali affrontando un ulteriore aspetto che deve essere tenuto presente per contribuire a costruire un'effettiva protezione dei dati personali nella società dell'informazione del nuovo millennio, nella società digitale; aspetto che esula da un discorso prettamente giuridico, ma rientra in quello che è il presupposto di qualsiasi regolamentazione normativa e interpretazione giurisprudenziale: la conoscenza della realtà su cui la norma deve agire, che in questo caso non è solo tecnologica (ed oggetto quindi dello

[26] La Corte di Giustizia afferma poi che «il diritto di chiunque a chiedere il risarcimento di un danno rafforza l'operatività delle norme di protezione previste da tale Regolamento ed è atto a scoraggiare la reiterazione di comportamenti illeciti», andando dunque oltre all'interpretazione della Cassazione italiana riportata nel testo sulla tesi del danno *in re ipsa* (ritenuta snaturare «la funzione del risarcimento, che verrebbe concesso non in conseguenza dell'effettivo accertamento di un danno, ma quale pena privata per un comportamento lesivo»: così Cass., Sez. Un., 11 novembre 2008, n. 26972), quasi ad affermare un risarcimento «rafforzativo» del sistema introdotto dall'art. 82 del Regolamento.

 ISBN 978-88-495-5334-5

studio del diritto dell'informatica), ma anche legata al complicato tema della protezione dei dati personali.

Complicato perché, a parte la complessità della materia in sé, la relativa disciplina può essere considerata un'anomalia «paradigmatica», creata principalmente dall'idea generalizzata che la vede come assolutamente inutile, burocratica, anzi addirittura dannosa per l'azione della P.A. o per chi vuole oggi fare impresa, insomma «qualcosa da cui difendersi».

Conseguenza di tale anomalia è stata la forte carenza negli anni di una generalizzata «cultura» della protezione dei dati personali, la disattenzione politica al problema, la scarsa sensibilità degli operatori del diritto, il basso livello di adeguamento alla normativa delle strutture dei vari titolari, privati ed anche pubblici.

Si può considerare esempio di questa anomalia proprio l'interpretazione giurisprudenziale delle norme che dispongono in tema di risarcimento del danno da trattamento illegittimo dei dati personali, analizzata nel precedente paragrafo. Infatti, la valutazione da parte del giudice sull'intensità del pregiudizio alla luce del principio di tolleranza, per poi escludere dalle ipotesi risarcitorie tutte quelle in cui il danno non patrimoniale lamentato si riveli essere un mero fastidio o un lieve disagio, può portare, in tale fattispecie, a pronunce non corrette a causa della non consapevolezza di quali danni si possano creare utilizzando informazioni relative agli individui nella società digitale: ad esempio, deve essere risarcito il danno causato dalla ricezione di mail contenenti comunicazioni commerciali non richieste (il c.d. *spamming*) ? Si può ritenere «tollerabile»? Anche tenendo presente che, dietro all'invio di un semplice messaggio di posta elettronica, che altrettanto semplicemente si può cancellare con un lievissimo fastidio, si riscontra un'attività illecita che parte da un vero e proprio «mercato» di indirizzi *mail*, numeri di cellulari, telefoni fissi, corrispondenti a soggetti profilati con precisione e quindi selezionati in maniera accurata, fino ad arrivare al loro utilizzo frequentemente finalizzato a perpetrare reati informatici, dal c.d. *phishing* ai veri e propri *data breach* (che nella maggioranza dei casi vengono realizzati proprio tramite allegati a innocui messaggi di posta elettronica)[27].

[27] Il «*phishing*» è un tipo di truffa effettuata utilizzando Internet e i suoi servizi, attraverso la quale chi agisce cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un soggetto affidabile in una comunicazione digitale. Invece un «*data breach*» è la «violazione della sicurezza del sistema del titolare che comporti, 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» (art. 4, punto 12, del Regolamento 679/2016): istituto disciplinato dagli artt. 33 e 34 della normativa europea, è finalizzato ad obbligare il titolare a denunciare all'Autorità Garante, e agli interessati, le infrazioni che subisce, permettendo in questo modo innanzitutto di avere notizia dell'evento (fino al Regolamento 2016/679 i *data breach* venivano tenuti nascosti da chi li subiva), e quindi realizzare una maggiore tutela dei soggetti i cui dati sono stati violati.

ISBN 978-88-495-5334-5

A tale proposito è la disciplina dettata dal Regolamento 2016/679 per la «violazione dei dati» a fornire ulteriori informazioni su quali potrebbero essere i danni conseguenti ad un trattamento illecito dei dati personali.

Il *considerando* 85 del Regolamento 2016/679, riferito al *data breach*, prevede infatti che i danni siano quelli «fisici, materiali o immateriali», e ne riporta alcuni (riferendosi all'interessato): la «perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie (…), pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale (…)»[28]. Come si può allora valutare, nell'esempio fatto, l'intensità del pregiudizio conseguente alla ricezione di mail di spamming senza tenere presenti le conseguenze dannose legate alla perdita di controllo dei propri dati personali o, peggio, all'eventuale usurpazione di identità? Operazione che certo non semplifica l'attività ermeneutica di chi deve poi decidere sulla richiesta di risarcimento.

In conclusione, alla luce delle considerazioni appena esposte, e valutate le difficoltà di trovare, nella realtà della protezione dei dati personali nella società digitale, il corretto bilanciamento tra il principio di solidarietà verso il danneggiato e quello di tolleranza imposto dal contesto sociale, si ritiene necessario una nuova riflessione da parte della giurisprudenza del nostro Paese sulla natura ed efficacia del sistema di responsabilità civile previsto dal Regolamento 2016/679, come interpretato dal suo orientamento maggioritario: al momento infatti l'analisi del solo danno cagionato all'interessato, e la valutazione della sua gravità, se effettuati in modo decontestualizzato dalle condotte complessive del titolare, e dalla realtà del trattamento dei dati personali, manifestano una mancata presa di consapevolezza del senso generale della normativa europea, privandola di parte della sua efficacia nella tutela di uno dei più importanti diritti inviolabili dell'individuo.

Riflessione, in particolare, che potrà però essere condotta in maniera adeguata solo successivamente ad una più accurata conoscenza della complessa normativa che consenta lo sviluppo di quella cultura della protezione dei dati personali di basilare importanza per una più corretta applicazione delle categorie tradizionali del diritto civile alle nuove tecnologie dell'informazione e della comunicazione.

[28] Risulta poi interessante riportare anche quanto indicato dal *considerando* 75 circa le tipologie di rischi che un trattamento di dati personali può realizzare: tra questi, ad esempio, le pericolosità connesse all'utilizzo delle informazioni relative agli individui «in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali»; oppure «se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori»; o ancora «se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati».

 ISBN 978-88-495-5334-5

Bibliografia: G. Buttarelli, *Banche dati e tutela della riservatezza: la privacy nella società dell'informazione*, Milano, 1997, pp. XIII-587; E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, pp. 1-289; Aa.Vv., *Codice della privacy e data protection*, a cura di R. D'Orazio, G. Finocchiaro e altri, Giuffré, Milano, 2021, pp. XXI-1795; Aa.Vv., *GDPR e normativa privacy*, a cura di E. Bellisario, G.M. Riccio, G. Scorza, Milanofiori, 2022, pp. XIII-1088.

ISBN 978-88-495-5334-5

Il Manuale approfondisce, in modo sistematico, il *cyberspazio* e gli istituti emersi dal mondo digitale e dell'informatica con le più rilevanti problematiche connesse al rapporto tra informatica e diritto, avendo particolare attenzione alle nuove sfide poste dall'innovazione tecnologica e dalla transizione digitale. Si intende offrire, con un taglio codicistico della materia, una sistemazione organica a tutti gli istituti che erompono dalla società digitale collocandoli all'interno delle categorie del codice civile permettendo, con questa schematizzazione, di dare allo studente ed all'operatore del diritto uno strumento chiaro con il quale approcciare al mondo digitale attraverso le categorie privatistiche.

Il Manuale di diritto privato dell'informatica è, quindi, suddiviso in sette parti attraverso le quali lo studente e gli operatori del diritto possono approfondire i temi del mondo digitale partendo dall'ordinamento giuridico, per poi approfondire la persona, i diritti reali del terzo millennio, il contratto ed i singoli contratti, le responsabilità civili in rete e le tutele. Si approfondiscono inoltre i temi di maggiore momento quali le nuove realtà dei metaversi, i *big data* e Internet *of things*, l'Intelligenza artificiale, i *Non Fungible Token*, i *social networks*, la *blockchain* e gli *smart contract* e *cloud computing*, mentre sono esclusi i profili di diritto del lavoro.

L'impostazione dei singoli contributi, corredati da indicazioni bibliografiche essenziali e da note esplicative, è particolarmente attenta alle finalità didattiche ma, al contempo, risulta di sicura utilità anche per gli operatori del diritto sia teorici che pratici che desiderano inquadrare in modo immediato i nuovi istituti emersi dalla realtà digitale all'interno delle categorie codicistiche.

Roberto Bocchini è ordinario di Diritto Privato dell'Università degli Studi di Napoli Parthenope. Attualmente è Prorettore ai rapporti con le Imprese, gli Enti pubblici, gli Ordini professionali e agli affari giuridici, ed è componente del collegio dei docenti del dottorato di ricerca in «Il diritto dei servizi nell'ordinamento italiano ed europeo».

È *Principal Investigator* del PRIN 2020 dal titolo «E-Agorà - Efficienza economica e tutela dei diritti degli utenti dei servizi. Innovazione tecnologica e condivisione dei servizi nel mondo digitale».

Ha insegnato nelle Università di Messina e presso la Libera Università Mediterranea di Bari.

I principali temi di ricerca spaziano dal diritto dei servizi in Italia al diritto dell'informatica, dai consumatori ai contratti, dalla famiglia alle obbligazioni. È curatore di diverse opere a rilevanza nazionale.

8423121230

MANUALE DI DIRITTO DELL'INFORMATICA

ESI

Questo volume, sprovvisto del talloncino a fronte, è da considerarsi copia saggio gratuito esente da IVA (art. 2, c. 3, lett. d, DPR 633/1972)

€ 96,00

ISBN 978-88-495-5334-5

9 788849 553345