JUS CIVILE

CARMELITA CAMARDI

Professore ordinario di Diritto privato – Università Ca' Foscari di Venezia

NOTE CRITICHE IN TEMA DI DANNO DA ILLECITO TRATTAMENTO DEI DATI PERSONALI

SOMMARIO: *1. La responsabilità per danni da trattamento illecito dei dati personali nella complessità ordinamentale. – 2. L'art. 82 del Regolamento UE 2016/679 e le altre norme che delineano ipotesi di danni causati da trattamenti illeciti dei dati personali. – 3. Le questioni interpretative. Imputazione della responsabilità e prova liberatoria. – 4. Segue. Ingiustizia del danno e risarcimento del danno non patrimoniale. – 5. Ancora sull'illecito trattamento dei dati personali nell'art. 82 del GDPR. Dogmatica interna e prospettiva (dogmatica) europea. Relativizzazione della tutela aquiliana nella complessità ordinamentale. – 6. Tramonto della responsabilità aquiliana?*

1. – Come noto a tutti, l'*enforcement* della disciplina di protezione dei dati personali, realizzato da ultimo con l'entrata in vigore del GDPR, ha riaperto il fronte tormentato della responsabilità civile e la questione del risarcimento del danno (patrimoniale e) non patrimoniale a favore dell'interessato che fosse caduto vittima di comportamenti scorretti e/o illeciti compiuti dal titolare del trattamento o del responsabile.

E sebbene questo profilo della complessa disciplina della *data protection* non sia il più controverso (se si pensa a quanto lo sia invece il profilo della natura giuridica dei dati personali e poi dei mega dati); mentre nel GDPR, come già nel Codice della privacy, il tema è disciplinato sia sul piano dell'imputazione della responsabilità che su quello del risarcimento del danno; ciononostante il contenzioso sorto in materia non ha mancato di riaprire i tradizionali dilemmi dell'istituto aquiliano.

Ciò con particolare riguardo al profilo del risarcimento del danno non patrimoniale, il quale – nella sua permanente complessità – ha nuovamente chiamato con sé il tema dell'ingiustizia del danno, che ha chiamato con sé quello della rilevanza della distinzione tra danno evento e danno conseguenza, e prima ancora quello della individuazione dell'interesse protetto o del bene della vita la cui lesione deve essere provata per essere

risarcita, (anche) quando la norma violata protegge e dà forma ad un diritto costituzionalmente garantito e addirittura ad un diritto fondamentale della persona, secondo le Carte dei diritti a pieno titolo entrate nei nostri sistemi giuridici.

Ed è così che la giurisprudenza si è ri-prodotta nei consueti contrasti che da sempre hanno accompagnato le riflessioni sul danno alla persona, con riferimento alla formulazione limitativa del risarcimento del danno non patrimoniale di cui all'art. 2059 e alla sua lettura costituzionalmente orientata.

Non intendo affrontare immediatamente e direttamente questo dibattito, e la specifica questione formale nella quale esso principalmente si sintetizza: quella cioè se il danno da violazione delle norme sul trattamento dei dati personali sia *in re ipsa*, e se occorra una qualche prova in tal senso da parte dell'interessato. Esaminerò rapidamente più avanti le decisioni, i commenti e la letteratura che hanno cercato di mediare fra i vari orientamenti e mettere un punto fermo.

Mi interessa di più, invece, allo scopo di fornire un contributo che non sia ripetitivo al tema dei nuovi danni, svolgere qualche osservazione generale e di contesto, per comprendere invero – trattandosi di un danno alla persona – come la persona si ponga effettivamente nel contesto dell'attività professionale di elaborazione e circolazione dei dati dominata da grandi *players* privati e comunque da soggetti istituzionali; quale sia lo statuto dei suoi diritti nel sistema giuridico che governa l'informazione e le informazioni, nel quale si muovono anche soggetti pubblici; e quale sia – in senso ampio – l'insieme dei rischi e dei danni, ovvero, in altri termini, l'offensività individuale e sociale del "mercato dei dati" e delle informazioni rispetto alle persone, per indagare se la dimensione prettamente individuale della responsabilità civile sia o no l'unico luogo nel quale trovare un rimedio per gli effetti dannosi che l'attività professionale di produzione, elaborazione e circolazione dei dati produce nella società contemporanea.

Non sembra esservi dubbio infatti sulla circostanza per la quale l'avvento della società e del mercato digitali rappresenti un fenomeno di trasformazione sociale di importanza pari a quello generato a suo tempo dalla rivoluzione industriale di massa [1]. E così come allora la responsabilità civile è stata costretta a misurarsi con i danni (tipicamente anonimi e inevitabili) da prodotti difettosi, oggi essa è costretta a misurarsi con i danni da trattamento illecito dei dati personali. E se quelli hanno indotto ad un complessivo ripensamento del sotto-sistema aquiliano, a partire dalla considerazione dell'attività produtti-

[1] Riferimenti e considerazioni assai esplicativi in A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Milano, 2020, pp. 1-28 ss.

va fonte dei danni come attività di per sé rischiosa se non pericolosa, e quindi fonte di responsabilità "senza colpa" (come poi è avvenuto con la responsabilità per danno ambientale); la fenomenologia dei danni da trattamento illecito dei dati personali può indurre ad un ulteriore ripensamento dei rimedi aquiliani, anche in altra direzione, ma a partire però dallo stesso presupposto teorico – concettuale: quello della inevitabile *pericolosità* dell'attività che è alla base degli effetti dannosi [2]. Ciò che del resto il Codice della privacy affermava a chiare lettere, quando riportava la responsabilità del titolare del trattamento alla fattispecie dell'art. 2050 cod. civ. [3]. Il GDPR non contiene un simile riferimento, né potrebbe in ragione della matrice europea della sua genesi, ma la disciplina offerta della fattispecie di responsabilità nell'art. 82 ed in tutte le norme ad esso collegate non lascia molti dubbi sul fatto che la *ratio* accolta in tema di imputazione della responsabilità si collochi in quella prospettiva.

Ma non solo di questo si tratta. Come già nel periodo di affermazione della produzione industriale di massa, ma forse molto più che allora, l'economia dei dati presenta un carattere particolarmente invasivo e massivo, si muove cioè su larga scala e in maniera fortemente intrusiva. Il che comporta che la produzione di effetti dannosi non si sostanzia (soltanto) nella diffusione/moltiplicazione quantitativa di danni individuali, ma si manifesta – qualitativamente in maniera diversa – nella produzione di danni *per definizione* seriali e massivi, che investono cioè sistemicamente serie indefinite e/o categorie individuate ma pur sempre indefinite di soggetti. E come tali certamente impegnano il sistema della responsabilità civile in una maniera del tutto nuova, mentre chiamano in causa anche altre strategie di protezione maggiormente incentrate su logiche preventive [4].

E però, a fronte di queste spiccate analogie strutturali, l'economia dei dati esprime la

---

[2] Indicazioni in A. MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, in *NLCC*, 1/2017, p. 144; nonché, per un quadro completo, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di A. MANTELERO e D. POLETTI, Pisa, 2018, in particolare p. 289 ss. Sulle trasformazioni delle funzioni della responsabilità extracontrattuale si vedano le pagine sempre illuminanti di P. TRIMARCHI, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2019, pp. 3-43 ss.; e quelle di C. CASTRONOVO, *Responsabilità civile*, Milano, 2018, p. 3 ss.; nonché il ricco volume *La responsabilità d'impresa*, a cura di G. ALPA, G. CONTE, Milano, 2015, in particolare i contributi di G. ALPA, *La responsabilità d'impresa nel terzo millennio*, p. 1 ss., e quello di G. RESTA, A. SALERNO, *La responsabilità civile per il trattamento dei dati personali*, p. 643 ss.

[3] *Ar*. FUSARO, *Attività pericolose e dintorni. Nuove applicazioni dell'art. 2050 c.c.*, in *Riv. dir. civ.*, 2013, p. 1337; C. BALDASSARRE, *Protezione dei dati personali ed art. 2050 c.c.*, in *Danno e resp.*, 2013, p. 4 ss.

[4] Coglie il fenomeno, e ne evidenzia gli aspetti formali, P. TRIMARCHI, *La responsabilità civile*, cit., p. 65 ss.

sua peculiarità, sotto il profilo dei danni e della sua pericolosità, attraverso un elemento che mancava e manca nel contesto del danno "industriale" da prodotti, e in fondo anche in quello del danno ambientale. Ed infatti, seppur queste due tipologie di danno toccano anche interessi legati alla persona (primo fra tutti, la salute), i danni generati dalle performance anche fisiologiche dell'economia digitale coinvolgono elettivamente, e in una maniera diretta e imprescindibile (oltre che subdola), la *persona in quanto tale*, la sua identità, la sua dignità, e ciò per la natura indiscussa – ancorché doppia e ambigua – dei "beni" sui quali il danno si produce: per l'appunto i *dati idonei a identificare la persona,* risorse che non perdono mai questo loro legame con la persona, nemmeno quando intraprendono in rete i flussi circolatori, di trattamento e rielaborazione cui grandi e piccoli *players* li sottopongono [5].

Questa constatazione, qualora intesa in senso pieno, potrebbe in teoria essere posta alla base dell'idea per la quale la violazione delle regole sul corretto trattamento dei dati personali costituisce di per sé un illecito *non iure* e *contra ius*: per cui non solo l'ingiustizia, ma lo stesso danno sarebbero *in re ipsa* inclusi nello stesso comportamento illecito, e null'altro l'interessato dovrebbe provare ai fini del risarcimento del danno non patrimoniale alla sua persona che non sia la violazione della regola di trattamento.

In altre parole, e mantenendoci ancora in una fase di mera anticipazione delle questioni tecniche proprie della disciplina del risarcimento danni posta dal GDPR, quest'ultima non dovrebbe comportare – in teoria – alcun ripensamento circa la dogmatica difensiva che ha caratterizzato le prese di posizione della dottrina civilistica agli albori della disciplina sulla *privacy*, quando si diceva in primis che i valori personali, una volta lesi, non sono traducibili in una somma di denaro; e poi che l'evento dannoso consiste nell'esplicazione della stessa condotta vietata e il danno si identifica con la stessa antigiuridicità della condotta [6]. Anzi l'aggressività specifica dell'industria digitale finirebbe per rafforzare questa dogmatica e le sue conseguenze applicative.

Sennonché, una tale opzione dogmatica, seppur mossa dal nobile e condivisibile in-

---

[5] Indicazioni esaustive in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. ALPA, *La proprietà dei dati personali*, in *Persona e mercato dei dati. Riflessione su GDPR*, a cura di N.Z. GALGANO, 2019, p. 9 ss. Ma vedi anche il parere del GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali,* reperibile anche nella pagina *https://www.ù garanteprivacy.it/documents/10160/10704/ARTICOLO+29+-+WP+136.pdf.*

[6] Per questa impostazione, vedi le eleganti pagine ancora fondamentali di D. MESSINETTI, *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, in *RCDP*, 2006, in particolare p. 550 ss.; ma già ID., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, *ibidem*, 1998, p. 339.

tento di preservare sempre e comunque la persona dagli effetti lesivi indotti dallo sviluppo dell'industria come della tecnologia e del mercato, non potrebbe a nostro avviso riproporsi tale e quale oggi come ieri, se non altro perché la considerazione giuridica del valore della persona, e il suo stesso statuto, hanno assunto una dimensione complessa, irriducibile al conflitto tra riservatezza del singolo e interesse alla circolazione delle informazione.

In primo luogo, infatti, occorrerebbe ricontestualizzare il valore della persona con riferimento al corredo dei diritti individuati dal GDPR nel quadro normativo complessivo dallo stesso introdotto, alla luce del principio per il quale "*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*". Principio che convive con quello per il quale il regolamento valorizza il diritto alla "protezione dei dati personali", ma che sdogana una buona dose dei rischi indotti dall'economia digitale come rischi fisiologici che la società e i singoli devono assumersi, quale corrispettivo degli immensi vantaggi che la stessa è in grado di generare [7]. Alla luce di questa combinazione formale di interessi, assume più che mai valore di teoria generale la considerazione per la quale l'ingiustizia del danno, che delinea l'ambito della responsabilità civile, va determinata "in base a una valutazione comparativa dell'interesse leso e dell'attività lesiva", dei "poteri e permessi" spettanti alle parti potenziali del conflitto, in base a "considerazioni di efficienza e di giustizia" [8].

In secondo luogo ma parallelamente, lo statuto della persona si arricchisce di altri diritti, legati non tanto alla dimensione prettamente individualistica o identitaria del singolo, quanto alla sua dimensione sociale e di cittadinanza piena e partecipativa. Alludiamo agli sviluppi del diritto alla trasparenza, paralleli tutt'altro che casualmente agli sviluppi del diritto alla riservatezza e al controllo dei propri dati personali, i quali hanno preso la forma di un principio organizzativo dell'attività della P.A., attraverso normative che, con strumenti che vanno dall'obbligo di pubblicità di taluni dati all'accesso civico, istituiscono una problematica convivenza – in termini di reciprocità – tra il diritto del singolo a tenere riservati i propri dati e l'opposto diritto degli altri a conoscerli. Un singolare con-

[7] Per questi profili, V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. dell'inf. e dell'informatica*, 2018, 4, p. 689; F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, p. 190; nonché il nostro *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, 3, p. 499.

[8] Così P. TRIMARCHI, *La responsabilità civile*, cit., pp. 43-44.

nubio tra segreto e memoria, tra riservatezza e conoscenza, che richiede altrettanta capacità di mediazione pratico-applicativa nel giudicare caso per caso se il trattamento e la diffusione di certi dati da parte della P.A. sia corretto e lecito, in ragione del rispetto di quella specifica normativa di trasparenza; o sia tutto al contrario scorretto e illecito in ragione della normativa sulla privacy. Con evidenti conseguenze sulla possibilità di configurare o meno in quell'atto della P.A. un illecito produttivo di danno ingiusto [9]

Ora, in che modo questa complessità influisce sulla configurazione della fattispecie di illecito aquiliano nella materia del trattamento e della circolazione dei dati è questione non semplice da risolvere, ma che merita comunque di essere indagata.

A questo scopo, è però necessario in via preliminare esaminare rapidamente l'attuale disciplina della fattispecie configurata nel GDPR.

2. – La disposizione regolamentare che espressamente disegna la fattispecie di illecito trattamento dei dati personali oggi vigente nell'Unione europea – l'art. 82 del GDPR – stabilisce quanto segue: "*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*". Dopo aver graduato la distribuzione della responsabilità fra titolare e responsabile del trattamento [10], il comma 3 dispone poi 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*".

Se questa è la fattispecie nei sui elementi costitutivi essenziali, dati dalla definizione della condotta illecita (la violazione del regolamento); dalla individuazione del danno risarcibile (materiale e immateriale, nel linguaggio *sdogmatizzato* dell'UE); nonché dal criterio di imputazione della responsabilità (oggettiva o per colpa presunta), salvo precisare il contenuto della prova liberatoria; altre disposizioni, unitamente agli immancabili considerando, arricchiscono il quadro con contenuti di non poco rilievo.

Innanzitutto la definizione n. 12 dell'art. 4, che introduce il concetto di *violazione dei dati personali*, come violazione di *sicurezza* che comporti "accidentalmente o in modo illecito la *distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'acces-*

[9] Su questo tema si avanti nel testo, il par.5. Utilissima in proposito la lettura di E. CARLONI, M. FALCONE, *L'equilibrio necessario. Principi e modelli di bilanciamento tra trasparenza e privacy*, in *Diritto pubblico*, 2017, 3, p. 723.

[10] A. MANTELERO, *Gli autori del trattamento dati: titolare e responsabile*, in *Giur. it*., 2019, p. 2799.

so ai dati personali trasmessi, conservati o comunque trattati". È abbastanza ovvio che il concetto sia un derivato sintetico dei fenomeni specificamente indicati come fattori di rischio che incombono sul titolare del trattamento ed in ragione delle caratteristiche dell'attività di ricerca, elaborazione e trattamento dei dati. Lavorare con i dati si può, ma in sicurezza, come dispone la sezione seconda del Regolamento, a partire dall'art. 32, con norme minuziose già richiamate dalla definizione dell'art. 4 citata che valgono a qualificare l'attività di trattamento come attività per definizione *rischiosa*, e individuano poi tali rischi in quelle circostanze (distruzione, perdita, ecc.) che possono conseguire ad una condotta illecita ma anche ad un incidente.

Ma ciò non è tutto. Il considerando n. 85 completa la costruzione della fattispecie sotto il profilo della individuazione del danno, aggiungendo che dalla violazione della sicurezza dei dati, che già produce – dobbiamo supporre – la lesione di un interesse protetto, possono scaturire "danni specifici" ulteriori (danni-conseguenza, si direbbe), consistenti nella violazione di libertà e diritti fondamentali, ivi menzionati come ipotesi di danni materiali e immateriali e ricondotti al diritto di non essere discriminati, all'identità, alla reputazione, ecc. [11].

Insomma, il quadro disegnato è confermato essere quello di un'attività ad alto rischio, in conseguenza del "pericolo" generato dall'elaborazione dei dati e dalla delicatezza della loro conservazione in stato di integrità. Anzi, più esattamente dovrebbe parlarsi di attività pericolosa "per la natura dei mezzi adoperati", *avente dunque il potenziale di causare danni*, e rispetto alla quale è alta la *probabilità* che si verifichi un evento in grado di causare un danno alle persone. Cioè *è alto il rischio*, tanto è vero che il regolamento prevede, anche qui a chiare lettere, l'importanza di una valutazione preventiva di impatto del trattamento sulla protezione dei dati, per valutare probabilità e gravità del relativo rischio (Sez. 3, artt. 35 ss.); e correlativamente vari obblighi di notifica e comunicazione delle violazioni della sicurezza che si siano in concreto verificate. Ma prevede soprattutto che il titolare e il responsabile del trattamento mettano in atto tutte le misure tecniche

[11] A commento delle disposizioni citate del GDPR si vedano M. RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo Regolamento*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. FINOCCHIARO, Bologna, 2017; G.M. RICCIO, *Diritto al risarcimento e responsabilità*, in *GDPR e normativa privacy. Commentario*, a cura di G.M. RICCIO, G. SCORZA e E. BELISARIO, sub *art.* 82, Milano, 2018; F. BILOTTA, *La responsabilità civile nel trattamento dei dati personal*i, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. PANETTA, Milano, 2019; E. TOSI, *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privac*y, Milano, 2019, p. 624 ss.

e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio.

Ciò che infine si riassume nella prescrizione di tutte quelle condotte e misure organizzative preventive e precauzionali che rientrano nel principio di *accountability*, formalizzato spiccatamente negli artt. 24 e 32, ma presente in moltissime altre norme del regolamento, incluse quelle che suggeriscono modalità per garantire anche l'attuazione del secondo aspetto del principio, quello segnatamente inteso a fornire le prove di aver adottato le più appropriate misure di sicurezza [12].

La disciplina da ultimo menzionata è di fondamentale rilievo ai fini della corretta individuazione della fattispecie di responsabilità per danno da illecito trattamento dei dati personali. Essa infatti contribuisce a tipizzare, seppur non in maniera chiusa né definitiva, le condotte dalla violazione delle quali può scaturire il danno ingiusto e la responsabilità dei soggetti del trattamento. Queste sono costituite dalle attività di trattamento che vengono svolte in spregio allo statuto protettivo dell'interessato in questa materia, quindi in spregio al consenso o senza altra base idonea, ovvero in violazione dei principi posti per la legittimità del trattamento agli artt. 5 e 6, o dei diritti dell'interessato *ex* artt. 12 ss. e fino agli artt. 22 e 23 [13]. E sono costitute altresì dalle condotte poste in violazione della normativa sulla sicurezza dei dati nel senso più ampio del termine, e alla luce del principio dell'*accountability*.

La violazione di una di queste norme dà luogo ad una condotta illecita.

Con riferimento al danno, lo si specifica ulteriormente, a parte l'espressa previsione della risarcibilità del danno patrimoniale e del danno non patrimoniale, i considerando 75 e 85 contengono un vero e proprio catalogo di conseguenze dannose, articolato su due livelli. Il primo relativo ai diritti fondamentali della persona che possono risultare lesi dalla condotta illecita, individuati in quelli che conosciamo e che tipicamente trovano protezione attraverso la responsabilità aquiliana (identità, reputazione, riservatezza, ecc.). Il secondo, concettualmente diverso se importato nello stile dogmatico italiano, relativo alle conseguenze dannose vere e proprie attraverso le quali si manifesta sul piano non patrimoniale la lesione del diritto: dalla decifratura non autorizzata della pseudonimizzazione, alla perdita di controllo di alcuni dati che rende possibile all'usurpatore assumere l'identità dell'interessato, alla discriminazione (se i dati dispersi rivelano origini razziali oppure orientamenti religiosi o sessuali), alla maggiore vulnerabilità se si tratta

[12] G. FINOCCHIARO, *Il principio di accountability*, in *Giur. it*., 2019, pp. 2778-2782 ss.; D. BARBIERATO, *Trattamento dei dati personali e "nuova" responsabilità civile*, in *Resp. civ. e prev*., 2019, 6, p. 2151.

[13] F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it*., 2019, p. 2789.

di soggetti "deboli" (minori, ad esempio), alla perdita della propria serenità di vita se si tratta di dati relativi alla propria abitazione o ai propri spostamenti utilizzati per una martellante azione di marketing [14].

Quanto al danno patrimoniale, di scontato riconoscimento, anche questo può concretizzarsi in perdite economiche o finanziarie se taluni dati raccolti in occasione di certe circostanze sono poi rielaborati e utilizzati in circostanze economiche diverse, e può essere questo il caso delle profilazioni di merito non aggiornate o non adeguatamente realizzate, che possono influire negativamente, ad esempio, in una selezione professionale competitiva per talune mansioni, nell'ottenimento di finanziamenti bancari sul piano del merito creditizio, e così via [15].

Quanto al danno non patrimoniale, risulterebbero più che ampiamente soddisfatte almeno le condizioni di operatività di cui all'art. 2059 cod. civ., per essere le norme citate del tutto chiare nel consentirne il risarcimento.

Sembrano perciò risultare – almeno in teoria – ampiamente soddisfatti tutti i requisiti generali della fattispecie aquiliana, avendo il complesso delle citate disposizioni delineato sia gli elementi rilevanti della condotta di cui rispondere, sia quelli della lesione ovvero del danno ingiusto [16]. E tuttavia sulla situazione pesano dubbi e incertezze interpretativi, in parte derivanti dalle formulazioni normative; in parte generati dalle applicazioni giurisprudenziali e dalle non sopite controversie dottrinali.

3. – Una prima questione concerne il criterio di imputazione della responsabilità del titolare del trattamento e degli altri soggetti eventualmente chiamati a rispondere dei danni per illecito trattamento dei dati personali. Ci si occupa in questa sede della posizione del titolare, che è comunque responsabile in via generale per qualsiasi trattamento

---

[14] S. THOBANI, *Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale*, in *Giur. it.*, 7, 2017, p. 1539.

[15] Su questi temi, A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 413; C. TABARRINI, *Comprendere la "Big Mind". Il GDPR sana il divario di intelligibilità uomo-macchina?*, in *Dir. informazione e informatica*, 2019, 2, p. 555.

[16] Per un primo approccio sintetico, R. CATERINA, S. THOBANI, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, p. 2805; A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Europa e dir. priv.*, 2018, p. 293 e *passim*; M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 1017.

svolto direttamente o tramite terzi (C74) [17]. E ci si occupa più ampiamente della responsabilità derivante da quelle violazioni del regolamento che concernono la sicurezza dei dati, piuttosto che il rispetto dei diritti dell'interessato. In tali ultimi casi, infatti, l'imputazione della responsabilità al titolare del trattamento va da sé, nel senso che accertata in fatto la violazione della regola che impone la richiesta del consenso dell'interessato o che obbliga alla rettifica del dato o all'informazione, è più difficile immaginare che il titolare possa elaborare una dimostrazione di non imputabilità, trattandosi di condotte dovute e poste a base della legittimità del trattamento. A meno che il titolare non contesti proprio il compimento in quel caso della condotta che l'interessato lamenta in quanto illecita (ad esempio, avere effettuato il trattamento su altra base; avere già effettuato la rettifica, ecc.) [18].

Diversamente invece si pone la questione per i casi di violazione delle regole di sicurezza o altre analoghe regole organizzative dell'attività.

Come si accennava, mentre l'art. 15 del Codice della privacy espressamente si richiamava all'art. 2050 cod. civ., istituendo un regime di responsabilità "senza colpa", che va oltre la semplice inversione dell'onere della prova, e che sembra riconducibile al modello della responsabilità per rischio "evitabile" [19]; la formula dell'art. 82 del GDPR libera il soggetto chiamato a rispondere del danno solo se dimostra "*che l'evento dannoso non gli è in alcun modo imputabile*". Una formula non coincidente con quella codicistica citata, ma che indubitabilmente la richiama, se l'art. 82 viene inteso alla luce di tutte le disposizioni del GDPR che sottolineano il carattere *pericoloso* dell'attività di trattamento dati e istituiscono un conseguente approccio basato "sul rischio". Sicché da questo punto di vista non dovrebbe essere difficile sostenere che il titolare del trattamento è soggetto ad un regime di responsabilità oggettiva da impresa "pericolosa".

Ma seppur si volesse evitare un ragionamento di questo tipo, basato su una lettura

---

[17] R. CATERINA, S. THOBANI, *Il diritto al risarcimento dei danni*, cit., p. 2806.

[18] M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 179.

[19] Sul modello dell'art. 2050 si veda in generale, P. TRIMARCHI, *La responsabilità civile*, cit., p. 411; C. CASTRONOVO, *Responsabilità civile*, cit., p. 439. Sull'art. 15 citato si vedano invece E. NAVARRETTA, *Commento* sub *art. 11 del d.lgs. 20 giugno 2003, n. 196*, in *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, a cura di C.M. BIANCA, F.D. BUSNELLI, I, Padova, Cedam, 2007, p. 241; G. COMANDÈ, *Commento sub art. 15, comma 1*, *ibidem*, p. 362; E. BARGELLI, *Commento sub art. 15, comma 2, ibidem*, p. 410; F. GRITTI, *La responsabilità civile nel trattamento dei dati personali*, in *Il codice del trattamento dei dati personali*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2007, p. 107.

domestica della norma europea [20], e si volesse invece leggere la norma del GDPR nell'ottica rovesciata di una *dogmatica europea*, quale emergente dalla normativa dell'UE e dalla giurisprudenza della Corte di Giustizia [21] i risultati apparentemente non cambierebbero di molto, ma andrebbero diversamente rappresentati.

Ed infatti, la responsabilità oggettiva del titolare del trattamento per tutte le lesioni "ingiuste" dei diritti e della posizione dell'interessato rappresenta il precipitato a valle di una visione a monte dell'attività del trattamento dati personali organizzata normativamente come attività libera ma *vigilata* e soprattutto "responsabile", ancor prima che un qualunque *data breach* si verifichi concretamente, sulla base del menzionato approccio basato sul rischio, ovvero del principio di *accountability*. Come è stato giustamente evidenziato, la responsabilità del titolare è – *ancor prima che per danni* – una responsabilità di ordine organizzativo, specie quanto alla sicurezza dei dati; alla stregua dell'art. 32, il titolare non deve limitarsi ad adottare le misure organizzative puntualmente stabilite in un certo disciplinare tecnico già predisposto, ma deve operare una preliminare valutazione di tutti gli elementi della sua attività (categorie di dati trattati, scopi del trattamento, livello di rischio, ecc.) e in base a questa adottare tutte le tecniche idonee a garantire un livello di sicurezza adeguato al rischio creato. Sotto questo profilo, gli artt. 35 e 36 del Regolamento individuano una procedura (di valutazione dell'incidenza complessiva del trattamento sui diritti delle persone e di preventiva consultazione dell'Autorità) la cui corretta esecuzione non può non venire all'attenzione nella fase dell'eventuale imputazione della responsabilità per danni. In più, il titolare deve premunirsi delle prove necessarie a dimostrare l'adozione di queste misure e la conformità della sua organizzazione al modello operativo del regolamento, e ciò, ancora una volta, indipendentemente dalla concreta causazione di un danno: tanto esplicitamente dispone il già menzionato art. 24 del GDPR [22].

Il tal senso, il contenuto della prova liberatoria prevista dall'art. 82 si presenta per

---

[20] Ad esempio ragionando sulla distinzione dogmatica tra imputazione a titolo di responsabilità oggettiva e imputazione a titolo di colpa presunta, secondo i modelli efficacemente descritti da D. BARBIERATO, *Trattamento dei dati personali*, cit., p. 2154 ss.

[21] In argomento, M.L. GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali,* Napoli, 2018, p. 99 ss., testo e note.

[22] Sugli oneri organizzativi imposti ai titolari di trattamento si vedano F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 775; R. TORINO, *La valutazione d'impatto* (*Data Protection Impact Assessment*, *ibidem*, p. 855; G. FINOCCHIARO, *Il principio di accountability*, cit., p. 2781 ss.; D. BARBIERATO, *Trattamento dei dati personali*, cit., p. 2153; A. MANTELERO, *Responsabilità e rischio nel Regolamento UE 2016/679*, cit., p. 156.

certi aspetti già precostituto, o meglio, trattandosi di una prova che richiede la dimostrazione della non imputabilità dell'evento dannoso "in alcun modo", essa implica che il titolare possa esibire certificazioni o documentazioni già in suo possesso concernenti l'adozione di tutte le misure tecniche di sicurezza intese a prevenire quell'evento dannoso lamentato dall'interessato, sulla base di una previa valutazione della probabilità del rischio. Sicché, allegati dall'interessato la violazione della regola, il danno e il relativo nesso causale materiale, il titolare risponderà dei danni derivanti dalla mancata adozione di (altre) misure tecnicamente possibili e proporzionate alle risultanze di quella valutazione, e non risponderà dei danni che erano stati esclusi da quella valutazione, se correttamente svolta, in quanto non prevedibili o altamente improbabili o non rimediabili allo stato dell'arte. Egli dunque non risponde del fortuito, classicamente inteso (ad esempio, un attacco hacker grave e generalizzato)[23], e nemmeno – sembra di poter ritenere – degli eventi dannosi non previamente stimabili sulla base di una elaborazione dell'approccio basato sul rischio condotta su parametri oggettivamente apprezzabili e proporzionati alla dimensione della sua attività[24]. Una prova quest'ultima, che non sembra propriamente coincidente con quella indicata nell'art. 2050 del nostro codice e che non sembra poter avere il contenuto limitato alla dimostrazione della propria diligenza nelle condotte attuative del trattamento[25]. Sembra più appropriato infatti ritenere che il titolare possa liberarsi dalla responsabilità dimostrando di aver effettuato una valutazione completa del rischio ed una conseguente organizzazione delle modalità del trattamento, consone allo scopo di evitare la produzione di quel danno.

4. – La complessità della fattispecie aquiliana, comunque costruita intorno al doppio binario della rilevanza della condotta illecita e dell'ingiustizia del danno causato dalla violazione della regola, torna a farsi pressante sul piano della individuazione dell'interesse leso e della definizione del danno risarcibile, quando si parla di danno non patrimoniale. Espressamente riconosciuto quest'ultimo nella espressione dell'art. 82 del GDPR nei termini di "danno *immateriale* causato da una violazione del presente regolamento".

---

[23] D. BARBIERATO, *Trattamento dei dati personali*, cit., *passim*.

[24] R. CATERINA, S. THOBANI, *Il diritto al risarcimento dei danni*, cit., p. 2808.

[25] Una sintesi del dibattito in S. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in *Regolare la tecnologia*, cit., p. 170 ss.; S. THOBANI, *Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento*, in *Giur. it*., 2019, 1, p. 43; M.L. GAMBINI, P*rincipio di responsabilità e tutela aquiliana dei dati personali*, cit., pp. 68 e 87 ss.

Come già detto, il regolamento non manca di esplicitare le tipologie di danno non patrimoniale potenzialmente generate da condotte illecite del titolare del trattamento, e molte di queste rispondono al modello tipico del danno non patrimoniale connesso alla lesione dei diritti della persona costituzionalmente protetti o fondamentali. Tanto è a dirsi per la lesione del diritto all'identità, all'onore, alla riservatezza e via dicendo; mentre dal punto di vista delle condotte più specificamente intese alla raccolta dei dati e al (controllo del) relativo trattamento altre lesioni possono in astratto configurarsi con riferimento ai diritti che il regolamento attribuisce all'interessato.

Ora, seppur non esattamente riferibile agli intenti e alla sistematica del regolamento, il problema che la dottrina e la giurisprudenza italiane si sono poste nella "trasposizione" della normativa europea nel nostro sistema presenta un forte appeal teorico-dogmatico, ma nel contempo una rilevanza pratica tutt'altro che banale, se solo si riflette sulle conseguenze economiche che l'allargare o il restringere la rilevanza del danno non patrimoniale può generare nella sfera giuridica e nei comportamenti dei titolari del trattamento. Ma qui, ancora una volta, può venire in gioco il metodo nell'interpretazione del diritto dell'UE, e la prospettiva – domestica o europea – dalla quale l'interprete muove nella lettura del GDPR.

Ed infatti, il quesito che i giudici italiani si pongono, già dai tempi del Codice della privacy, è se una volta realizzatasi la lesione del diritto della persona attraverso la violazione della regola di condotta che lo protegge da interferenze ed offese altrui, ciò non sia sufficiente a determinare contestualmente l'insorgenza di un danno non patrimoniale risarcibile, senza che l'interessato debba fornire ulteriori prove, ed in ragione della natura tutta speciale del diritto leso e del danno di cui si chiede ristoro: l'uno, diritto della persona non patrimonializzabile; l'altro, per sua natura liquidabile *già* in relazione alla gravità dell'illecito, e non ad una perdita emergente o a un mancato guadagno. Ciò che di solito si riassume nell'espressione per la quale in tali casi il danno non patrimoniale sarebbe *in re ipsa*. In altre parole, la lesione del diritto della persona rileva in sé e per sé, perché il danno consiste proprio nella lesione del diritto *personale*, e se non se ne potesse stabilire un ristoro, allora dovrebbe dirsi che l'ordinamento non è in grado apprestare tutela *ex post* ai diritti che più di altri protegge nella forma della *inviolabilità*: il che sarebbe un paradosso inaccettabile [26].

[26] Non è questa la sede per ripercorrere le vicende dottrinarie dell'illecito contro la persona e del risarcimento del danno non patrimoniale. Una sintesi efficace in G. PONZANELLI, *Certezze e incertezze nel danno alla persona*, in *Danno e resp*., 2020, I, p. 103: indicazioni generali in C. SCOGNAMIGLIO, *L'ingiustizia del danno (Art. 2043)* e P.G. MONATERI, *Il nuovo danno non patrimoniale. La nuova tassonomia del danno*

Sarebbe questo l'esito di quella dogmatica che si è in apertura di queste note definita come "difensiva", e alla quale si deve l'elegante ricostruzione per la quale il concetto di persona istituirebbe "un punto di vista omogeneo per la comprensione *sub specie juris* di una fenomenologia del reale non riconducibile al paradigma utilitarista proprio del mercato"; sicché, da tale punto di vista, il danno alla persona sarebbe portatore di una sua logica autonoma in quanto valore intrinseco della persona non ricostruibile attraverso una prestazione pecuniaria. Ciò porterebbe pertanto ad un mutamento o *sviamento* della funzione della responsabilità, da ritenersi orientata non più (soltanto) verso la riparazione, ma (anche) verso la deterrenza, perché l'evento dannoso in questi casi altro non sarebbe che la stessa condotta vietata *in sé*, cioè l'antigiuridicità della condotta in quanto tale! E ciò varrebbe specificamente proprio con riferimento ai danni non patrimoniali riconducibili alla violazione delle regole sul trattamento dei dati personali, attività la cui aggressività di immediato impatto sulla persona richiederebbe una conferma della concezione dei diritti personali come espressione di un *comando generale* rivolto a terzi affinché si astengano da ogni interferenza [27]. Insomma, il danno non sarebbe più il risultato prodotto dall'evento – e selezionato in base al criterio dell'ingiustizia – ma l'evento in sé stesso, il quale, in quanto offensivo della persona, non abbisognerebbe nemmeno di essere selezionato attraverso l'ingiustizia [28].

Sul piano pratico, come pure si accennava, è abbastanza evidente che una tale impostazione può sorreggere l'obbligazione di risarcimento del danno senza che alcun filtro, in termini di ingiustizia, si ponga tra la violazione della regola di condotta e il riconoscimento del diritto al risarcimento, e che pertanto il rischio delle conseguenze dannose della violazione sarebbe in tutti i casi a carico del titolare del trattamento, al quale nessuna possibilità di prova contraria sarebbe concessa, salvo quella di negare che l'evento sia accaduto, cioè dimostrare *in apicibus* che nemmeno c'è stata la condotta illecita. Il perimetro del risarcimento sarebbe quello della violazione della condotta e l'ammontare dei debiti risarcitori crescerebbe in via esponenziale.

---

alla persona, entrambi in Illecito e responsabilità civile, in *Trattato di diritto privato (diretto da M. Bessone)*, Torino, 2005, I, rispettivamente pp. 54 ss. e 277 ss.; P. TRIMARCHI, *La responsabilità civile*, cit., pp. 127-138 ss., 629 e 632 ss., ove l'A. non esclude che in alcune ipotesi un "danno-base non patrimoniale sussista sempre per la natura stessa dell'atto offensivo, salvo l'eventuale adeguamento del risarcimento …" (p. 633). Ma in altra sede l'illustre A. ricorda che "la natura del danno non patrimoniale consente di liquidarlo tenendo conto della gravità dell'atto illecito" (*op. cit*., p. 524).

[27] Il riferimento è ancora a D. MESSINETTI, *I nuovi danni. Modernità, complessità della prassi e pluralismo della nozione giuridica di danno*, cit., pp. 543-550 ss. e *passim*.

[28] D. MESSINETTI, *op. ult. cit.*, pp. 556-561.

A fronte della rigidità e ampiezza delle conseguenze generate da tale dogmatica difensiva, è ben noto che la dottrina e la giurisprudenza italiane hanno reagito, reintegrando in vario modo il danno non patrimoniale da illecito trattamento dei dati nella struttura della fattispecie aquiliana classica di cui all'art. 2043. E ciò secondo varie gradazioni.

In primo luogo affermando che il danno deve essere sempre dimostrato, non sottraendosi alla verifica della "gravità della lesione" e della "serietà del danno" medesimo; nel rispetto peraltro di un generale principio di tolleranza, se non di solidarietà [29]. Sicché i giudici vanno in tal caso alla ricerca di qualcosa di concreto da risarcire, che possa considerarsi conseguenza dell'evento dannoso e da questo "separabile" (il disagio, piuttosto che il fastidio, la vergogna, ecc.) [30].

In secondo luogo introducendo una presunzione di danno *in re ipsa*, la quale offrirebbe al titolare del trattamento il destro di fornire la prova contraria e di *dimostrare* la mancanza della gravità della lesione o della serietà del danno, con esclusione quindi dei danni bagatellari dal perimetro del risarcimento [31]. Una costruzione, questa, che sembra voler bilanciare la posizione delle parti, ma che finisce di fatto per privare di contenuto – almeno il più delle volte – la prova contraria offerta al danneggiante, il quale non si vede come possa dare dimostrazione della mancanza di stati d'animo che non gli appartengo-

---

[29] In tal senso Cass., 15 luglio 2014, n. 16133, in *Danno e resp*., 2015, 4, con *Commento di V. Ceccarelli*, *ibidem*, p. 343 e M. NITTI, *La valutazione della "gravità della lesione" e della "serietà del danno" nel risarcimento del danno non patrimoniale da violazione della privacy*, *ibidem*, p. 350. La decisione riporta il risarcimento del danno non patrimoniale nell'alveo della norma generale di cui all'art. 2043. Ma vedi già Trib. Napoli, 28 aprile 2003, in *NGCC*, 2004, I, p. 466 con nota di G.M. RICCIO, *Responsabilità da illecito trattamento dei dati personali e prova del danno non patrimoniale*, *ibidem*, p. 470.

[30] Nella controversia poi decisa dalla sentenza citata in nota precedente si discuteva della possibilità di risarcire il "disagio" subito dagli specializzandi dell'Università di Roma Tre per aver l'Ateneo reso possibile accedere ai loro file personali semplicemente digitando il nome su Google. Tale indiscriminata esposizione era stata ritenuta sufficiente dal Tribunale di 1° grado al fine di attribuire a ciascuno un risarcimento di 3.000,00 euro. La Suprema Corte cassa con rinvio, enunciando il principio per il quale l'applicazione dell'art. 15 del Codice della privacy non si sottrae alla verifica della "gravità della lesione" (concernente il diritto fondamentale offeso), e nemmeno a quella della "serietà del danno", cioè della perdita effettivamente subita dall'interessato a causa d quella lesione.

[31] Cass., 4 giugno 2018, n. 14242 e Cass., 8 gennaio 2019, n. 207, entrambe in *Corr.giur*., 2019, 5, pp. 625-626, con interessante nota critica di M.S. ESPOSITO, che mette a confronto le due decisioni, l'una circa la illiceità delle modalità di diffusione di un provvedimento contenente informazioni su un procedimento penale riguardante il destinatario; l'altra – di grande interesse – concernente il problema delle segnalazioni alla centrale dei rischi di dati rilevanti ai fini della concessione di un finanziamento. L'A. mette in rilievo come non sia ammissibile un giudizio in merito alla rilevanza ed entità deli interessi tutelati allorquando il risarcimento sia collegato alla violazione di diritti inviolabili della persona. La cd soglia di risarcibilità può essere impiegata semmai quale parametro per la determinazione dell'entità del risarcimento (*op. cit.*, p.633 ed ivi altra bibliografia).

no. Sicché ancora per consentirgli di ridurre le obbligazioni risarcitorie a suo carico gli si consente di dimostrare che il danno non è serio: prova che, a dire il vero, non attiene affatto all'ingiustizia del danno ma alla sua quantificazione [32].

5. – Ora, se si adotta la necessaria prospettiva del diritto dell'UE, e in particolare del Regolamento dati – atto immediatamente normativo in tutti gli ordinamenti di paesi membri, che necessita certamente di adattamento ma non di recepimento – non è certamente il caso di prender partito circa la riferita controversia in materia di danno non patrimoniale (e relativa prova) da illecito trattamento dei dati personali. E questo non perché si voglia rifuggire dall'onere che ad ogni interprete spetta di motivare la soluzione giuridica di un caso sulla base di argomenti di giustificazione sistematicamente accettabili, ragionevoli e controllabili. Ma perché ormai la soluzione del problema va tratta e argomentata sulla base innanzitutto del regolamento, salvo poi adattarla alle peculiarità formali del nostro ordinamento.

Ciò posto, occorre riprendere dove abbiamo lasciato, e cioè dal *testo* dell'art. 82, in

---

[32] In argomento, ed a nota di Cass. n. 14242/2018 indicata in nota precedente, S. THOBANI, *Il danno non patrimoniale da trattamento di dati tra danno presunto e danno evento*, in *Giur. it*., 2019, 1, p. 43. L'A. critica gli argomenti della Corte relativi alle due presunzioni che in tali fattispecie si applicherebbero in virtù del richiamo che il Codice della privacy operava all'art. 2050 cod. civ.: quella relativa all'imputazione della responsabilità, e quella relativa all'esistenza del danno: aventi la prima natura processuale e la seconda la diversa natura di cui all'art. 2727 cod. civ. Conclude affermando che la presunzione del danno in re ipsa poggia, in verità, sulla natura del diritto violato, l'onore o la dignità, la cui lesione lascia presumere sofferenze personali ulteriori, ma non potrebbe estendersi alla lesioni di altri diritti posti a tutela di interessi diversi (ad es., la mancata comunicazione all'interessato del nome del responsabile del trattamento, ovvero la prosecuzione del trattamento dei dati a fini di marketing nonostante l'opposizione dell'interessato). Ciò posto, la prova contraria, come si dice nel testo, non potrebbe che riguardare la serietà del danno, non la sua sussistenza (*op. cit*., p. 46). Più ampiamente sul tema si veda ancora S. THOBANI, *Il danno non patrimoniale da illecito trattamento dei danni personali*, in *Dir. inf e informatica*, 2017, p. 427, ove diffusamente l'A. articola il suo ragionamento sul tema della prova del danno non patrimoniale analizzando la ratio e la natura degli interessi tutelati dalle norme di protezione dell'interessato di fronte alla circolazione dei dato che lo riguardano, distinguendo la rilevanza della lesione dei diritti costituzionalmente tutelati (onore, riservatezza, identità, per la lesione dei quali non v'è altro da provare); da quella riguardanti invece altri diritti (di informazione, conoscenza ecc., per i quali "disturbi e fastidi" patiti andrebbero provati. Sulle oscillazioni della giurisprudenza e della dottrina si vedano anche F. DI CIOMMO, *La risarcibilità del danno non patrimoniale da illecito trattamento dei dati personali*, in *Danno e resp*., 2005, 7, p. 801; M. GAGLIARDI, *Commento* a Cass., 15 ottobre 2015, n. 20890, in *Danno e resp*., 2016, 4, p. 372; G. RAMACCIONI, *La protezione dei dati personali*, *Il tema/problema del risarcimento del danno non patrimoniale*, in *Danno e resp*, 2018, 6, p. 665; ID., LANGDELL, *Pound e il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali. La prasi italiana anche alla lice dell'entrata in vigore del Regolamento UE 2016/67*9, in *Regolare la tecnologia*, cit., p. 467.

combinazione con le altre norme che delineano il *contesto* nel quale si pongono gli obblighi di condotta la cui violazione dà luogo al risarcimento del danno "immateriale" a favore dell'interessato e a carico del titolare.

Non abbiamo mancato di rilevare come le disposizioni regolamentari siano tutt'altro che parche nell'individuare tutti gli elementi che in astratto compongono una fattispecie dannosa: la condotta vietata, l'evento dannoso conseguente, il danno risarcibile. Se si parte dall'idea per la quale nel contesto del diritto dell'UE i diritti della persona sono protetti alla stessa stregua dei diritti costituzionalmente garantiti; e se ancora, attraverso questo filtro interpretativo si legge nel GDPR il riconoscimento del modo specifico in cui essi si articolano di fronte alla complessità tecnica e alla pericolosità delle operazioni di trattamento dei dati personali, può nascere la tentazione di replicare – anche dal punto di vista del Regolamento – la logica assolutistica dei diritti della personalità e assecondarla attraverso il riconoscimento della rilevanza *in sé* delle violazioni delle regole imposte al titolare e al responsabile del trattamento, e pertanto l'immediata risarcibilità della *mera* lesione causata agli interessi protetti.

Non si vuol certamente dire che questa logica sarebbe irreplicabile o sconveniente in quanto tale, posto che in tal modo si assicura certamente alla persona la protezione più ampia possibile, insieme con l'aspettativa che la funzione di deterrenza contestualmente realizzata nei confronti dei titolari professionali di trattamento dati renda meno frequenti le occasioni di violazione della condotta e quindi di danno.

Il punto è però che non si può essere sicuri della replicabilità di quella logica nel *contesto* del GDPR, perché proprio questo contesto, sistematicamente inteso, sembrerebbe ispirato ad una *ratio* non perfettamente equivalente.

Ed infatti, a dispetto del suo tenore letterale ("*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*"), l'art. 82 del GDPR non può essere interpretato come se disponesse una piena coincidenza tra violazione di una norma del regolamento ed evento dannoso *di per sé* "ingiusto". E ciò per più di una ragione.

a) Innanzitutto, ai fini di una richiesta di risarcimento occorrerebbe verificare le norme la cui *ratio* sia quella di evitare danni materiali o immateriali ai soggetti interessati da un trattamento ai propri dati personali. E fra queste, in particolare, selezionare le norme intese a proteggere direttamente (come *bene della vita*) i diritti personalissimi costituzionalmente garantiti dall'altrui illecita interferenza. Non si può ignorare, infatti, che le norme regolatrici dell'attività di trattamento dei dati personali sono intese certo alla pro-

tezione dei diritti e delle libertà fondamentali delle persone fisiche, ma riconoscono altresì la legittimità e la pienezza del principio della libera circolazione dei dati – evidentemente in capo ai soggetti che la organizzano professionalmente –, al punto tale che – lo si rammenta di nuovo – il 3° comma dell'art. 1 del GDPR non fa mistero di affermare che "*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Ora, al momento della costruzione (e poi della verifica) dei requisiti di perfezionamento della fattispecie aquiliana, con riguardo al riconoscimento in concreto del danno non patrimoniale, non si può ignorare quell'affermazione di principio, a tenore della quale piuttosto sorge il dubbio che la protezione dei diritti e delle libertà fondamentali delle persone fisiche non rivesta più quella posizione di primazia che – ad esempio nella prima disciplina italiana di recepimento – vedeva una disposizione come quella di cui all'art. 1 della l. n. 675/1996 [33], assai prossima ad una concezione del tutto assolutistica della persona e dei suoi diritti.

Ciò posto, non si potrebbe nemmeno ritenere, senza incorrere in un errore metodologico assai grave, che la protezione dei diritti personali sia subordinata (integralmente o) anche soltanto fortemente alla realizzazione del principio della libera circolazione mercantile dei dati. Ma si può invece ricostruire una sistematica nella quale si accetta come ordinaria e inevitabile l'interferenza che (il principio del)la circolazione "mercantile" dei dati genera nella sfera personale delle persone fisiche; e però, proprio in ragione di ciò, si dispone che le attività di trattamento dati siano organizzate secondo le regole e i principi che – fra l'altro – si includono nel cd "approccio basato sul rischio" e nella regola diffusa dell'*accountability,* che devono connotare l'organizzazione dell'impresa del titolare del trattamento e dei suoi referenti. In questo quadro, peraltro, si spiega sia la previsione del consenso dell'interessato come una soltanto delle basi legittime del trattamento; sia l'espresso riferimento ad una attività di tipo contrattuale che include la "cessione" di dati personali, della quale l'interessato è parte, e per la quale rilascia un consenso anche di carattere negoziale (art. 6 GDPR). Attività di cui ovviamente il GDPR non si occupa, ma che è oggetto di altre normative europee (che lo richiamano), oltre che di una prassi fin troppo nota per essere qui menzionata [34].

---

[33] Lo ricorda V. RICCIUTO, *La patrimonializzazione dei dati personali*, cit., p. 5 (versione De Jure), il quale considera il testo della norma come "uno sforzo celebrativo e protettivo … mai visto prima in qualsiasi normativa riguardante i diritti della personalità".

[34] Sul punto, e sulla posizione che l'interessato assume nello "scambio" dei suoi dati contro servizi e be-

Tutto ciò permette forse di ricalibrare l'impostazione del problema e di riconoscere che la rappresentazione assolutistica della persona che funzionava da premessa logica di quella che più volte abbiamo denominato "dogmatica difensiva", andrebbe forse relativizzata, alla luce dell'ottica dichiaratamente mercantile e patrimonialistica del Regolamento [35]. Quest'ultimo certamente prende atto della consistenza del "mercato dei dati" e lo rende oggetto di una disciplina tipicamente regolatoria la quale, nel momento in cui ridimensiona i valori della persona in un contesto di "normale" circolazione anche volontaria dei dati personali come risorse dichiaratamente oggetto di un'attività di impresa, allenta la rilevanza dell'interferenza esterna sulla persona e riconfigura in questa chiave, inevitabilmente, l'istituto posto a presidio dei rimedi contro tale interferenza, e cioè la responsabilità aquiliana.

Di qui la possibile lettura della formulazione dell'art. 82, "*danno materiale o immateriale causato da una violazione*", quale riferimento alla sequenza: a)violazione della regola posta a protezione della persona e b) causazione di un danno come *conseguenza ulteriore* dell'illecito, *almeno tutte le volte in cui* non vi sia stata *una lesione diretta dei diritti della personalità costituzionalmente garantiti, dimostrata la quale spetta senz'altro all'interessato il risarcimento del danno non patrimoniale quale ristoro della lesione ingiusta del diritto*. Negli altri casi invece, quando la regola organizzativa violata non abbia quale ratio la tutela immediata e diretta di questi diritti, ma di quelli volti a garantire il controllo materiale della conservazione o circolazione dei propri dati, l'interessato dovrà provare la conseguenza dannosa riportata nella sua sfera personale, sotto forma di concreta compromissione della sua sfera di esistenza e secondo standard di medietà sociale, o *de minimis*, che rendono giustificabile il risarcimento [36]. Sono questi, ad esempio, i casi nei quali viene in gioco direttamente il principio della libera circolazione dei dati, per come configurato nel citato comma 3 dell'art. 1 del Regolamento; ed allora il bilan-

---

ni digitali, si veda il nostro Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali, in *Giustizia civile*, 2019, 3, p. 499; G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in *Annuario del Contratto 2018*, diretto da A. D'ANGELO, V. ROPPO, Torino, 2019, p. 125, ed ivi altre indicazioni bibliografiche.

[35] In argomento, V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., pp. 3-17 ss.

[36] Così ampiamente argomentando, S. THOBANI, *Il danno non patrimoniale da illecito trattamento dei danni personali*, cit., p. 433 ss. Sulla regola *de minimis*, in punto teorico, per tutti, P. TRIMARCHI, *La responsabilità civil*e, cit., p. 634, con riferimento a un generale principio di tolleranza "imposto dai limiti connaturali all'organizzazione giuridica".

ciamento di interessi si struttura tutto in questo contesto, ove pertanto nel nome di quel principio, per come le circostanze lo rendono evidente, può trovare spazio il diritto del titolare del trattamento all'utilizzo/diffusione dei dati, ovvero quello dell'interessato a bloccarne la circolazione [37].

Ma sono anche i casi nei quali lo stesso principio viene in gioco attraverso la violazione delle regole che richiedono il consenso dell'interessato, quando il titolare raccoglie dati ad esempio a fini statistici e di marketing, ovvero eccede le finalità del trattamento, ma senza che possa dirsi esservi stato un turbamento delle condizioni di esistenza dell'interessato, il quale potrà chiedere la cessazione della condotta illecita per aver questa violato il suo diritto al controllo della circolazione dei dati personali, ma non dovrebbe poter chiedere *anche* il ristoro del danno non patrimoniale se non in presenza di un fastidio, di un disagio personale che abbia un minimo di significatività. Ugualmente nei casi in cui il titolare non ha custodito e conservato adeguatamente i dati, ma alla perdita degli stessi non ha fatto seguito l'accesso di terzi non autorizzati [38].

In altre parole, in tutti i casi esemplificati, non è che non si possa predicare l'illiceità della condotta e la violazione di un interesse giuridicamente protetto: si vuol solo dire che l'interessato dispone certamente di tutti i rimedi previsti dal Regolamento per reagire alla violazione delle norme poste a presidio della liceità del trattamento ed a sua protezione, ma potrebbe *non disporre anche* del risarcimento del danno non patrimoniale qualora la lesione ingiusta non abbia concretamente provocato quel *quid pluris* di deprezzamento delle condizioni di vita che ne giustifica la concessione, ed in assenza del quale il risarcimento assumerebbe una funzione meramente punitiva incompatibile con i principi che regolano la libera circolazione dei dati come oggetto di un'attività pericolosa ma lecita, se non anche necessaria [39].

Questo assetto non può essere inteso come effetto di una strategia normativa di intenzionale riduzione del livello di tutela della persona in un ambito di rapporti così al tempo stesso delicato ed esteso. Quanto piuttosto come conseguenza della ricollocazione dei diritti della persona al controllo della circolazione dei propri dati personali in una più com-

---

[37] Sul tema del bilanciamento tra diritto all'oblio e diritto di cronaca, si veda da ultimo Cass., SS.UU., 22 luglio 2019, n. 19681, e già Cass., 3 aprile 2018, n. 8084, reperibile in *De Jure* con nota di I. Alagna.

[38] Casistica in S. THOBANI, *op. loc. ult. cit*.

[39] Esemplare il caso deciso negativamente da Cass., 8 febbraio 2017, n. 3311, con nota di S. THOBANI, *Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale*, in *Giur. it.*, 2017, 7, p. 1539, circa l'irrisarcibilità di un danno non patrimoniale causato dall'invio di 10 email indesiderate in tre anni.

plessa realtà che ha fatto della circolazione dei dati e della loro libera diffusione oggetto di attività e funzioni di rilevanza pubblica e/o istituzionale le quali, inevitabilmente, insidiano i confini (non della protezione, ma) entro i quali la persona può pretendere il rispetto del divieto assoluto di interferenza da parte di terzi nella sua sfera privata. Del resto che il diritto alla protezione dei dati personali non sia una "prerogativa assoluta" è affermato a chiare lettere nel Considerando 4 del citato Regolamento UE 2016/679 [40].

b) Ed è qui che viene in gioco un altro principio già menzionato in precedenza, *simmetrico* e *antagonista al principio della riservatezza*, che si affianca a quello della libera circolazione dei dati assunta quale oggetto di un'attività professionale di trattamento. È il principio generale della trasparenza [41] e della libera accessibilità di alcuni dati alla conoscenza dei quali il legislatore affida il compito di realizzare, volta a volta, interessi pubblici: siano questi legati alla necessità della trasparenza in senso stretto dell'azione amministrativa pubblica, quale suo modo *costituzionale* di essere correlato alla imparzialità e alla efficienza; siano questi legati alla necessità di evitare il dilagare di fenomeni corruttivi nella gestione dei contratti e degli investimenti pubblici. La doverosità della trasparenza, nel suo rilievo costituzionale e nella sua stretta connessione con il carattere democratico del nostro ordinamento, assegna a ciascun cittadino già dotato del diritto al-

[40] "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica". Un esempio, altamente discutibile, ma comunque di interesse teorico significativo sul piano del bilanciamento dei diritti è quello della controversia decisa dal Trib. Milano, 22 luglio 2009, in *Corriere giur*., 2010, 12, p. 1665, con nota di S. SICA, *Tutela dei dati personali e libertà religiosa quale possibile scriminante del trattamento illecito*, *ibidem*, p. 1669. Nella fattispecie il Tribunale esclude l'illiceità della condotta, rispetto all'art. 26 Codice privacy, di un coniuge il quale aveva fatto uso di dati personali sensibili della moglie, raccolti nell'ambito di sedute mediche, senza il di lei consenso e allo scopo di predisporre un parere tecnico da esibire nella causa di annullamento del matrimonio avanti al Tribunale ecclesiastico. I giudici ritengono che il diritto di autodeterminarsi nella propria sfera religiosa costituisca in questo caso valida esimente della illiceità della condotta, in quanto diritto di pari rango costituzionale rispetto a quello alla riservatezza.

[41] "*La trasparenza è intesa come accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. … Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino.*" Così si legge nel fondamentale art. 1 del d.lgs. 14 marzo 2013, n. 33.

la riservatezza, un contrapposto diritto alla conoscenza: e tale coesistenza fa sì che la strategia di protezione meramente difensiva della persona ceda il posto ad una strategia bilanciata disponibile a sacrificare la riservatezza per valorizzare il diritto di "sapere", a comprimere il diritto a limitare la circolazione dei propri dati per soddisfare quello opposto a renderli pubblici e disponibili [42].

Ed invero proprio dalla normativa sulla trasparenza si possono trarre spunti non privi di interesse e di impatto sulla tematica della protezione aquiliana dei dati. Come noto, l'art. 5 *bis* del d.lgs. n. 33 in materia di esclusione e limiti all'accesso civico dispone che "*L'accesso di cui all'articolo 5, comma 2, è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati: a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia; b) la libertà e la segretezza della corrispondenza; c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali*". La norma trova il suo ambito tecnico-applicativo specifico, dunque, nella motivazione che la P.A. può addurre per giustificare il diniego di accesso, allorquando si ritenga debba prevalere nel caso specifico il diritto alla protezione dei dati personali sull'opposto diritto a conoscere quelle informazioni. Ebbene, la lettera della norma costruisce tale possibile motivazione intorno alla dimostrazione del cosiddetto "pregiudizio concreto" che l'accesso arrecherebbe al diritto del singolo a tenere riservati quei dati specifici. Ora, le Linee guida previste dalla legge sulla trasparenza a carico dell'ANAC e d'intesa con il Garante [43], allo scopo di definire le "esclusioni e i limiti all'accesso civico di cui all'art. 5 del d.lgs. n. 33/2013", si sono occupate esattamente di costruire le linee argomentative che la P.A. deve seguire nel motivare il diniego all'accesso in ragione della protezione dei dati personali cui la richiesta del cittadino si rivol-

[42] Le modalità attraverso le quali la legge regolamenta la trasparenza sono molteplici. Si comincia dal (principio generale del) diritto di accesso ai documenti amministrativi, di cui alla legge sul procedimento amministrativo n. 241/1990; per passare attraverso gli obblighi di pubblicazione di una serie di dati da rendere accessibili in via immediata, e giungere fino all'accesso civico generalizzato anche a documenti ulteriori rispetto a quelli oggetto di pubblicazione e consentito senza necessità di alcuna motivazione specifica (*ex* d.lgs. n. 33/2013 e n. 97/2016). In ciascuno di questi casi sono sempre presenti norme di combinazione e bilanciamento, volte a proporzionare riservatezza e trasparenza, specie con riguardo ai dati sensibili e ai diritti in ragione dei quali l'accesso è richiesto. In argomento si legga il bel saggio di E. CARLONI, M. FALCONE, *L'equilibrio necessario. Principi e modelli di bilanciamento tra trasparenza e privacy*, cit., *passim*, particolarmente efficace nel dimostrare analiticamente e teoricamente come il principio della trasparenza si innervi tanto quanto il principio della riservatezza nella dimensione personalistica.

[43] E da questi approvate con delibera 28 dicembre 2016, n. 1309, consultabile nella pagina *https://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666.*

ge. Nel distinguere tra eccezioni assolute e semplici limiti di cui all'art. 5 bis sopra citato, si dispone che la PA non potrà opporre un diniego all'accesso basato sul rischio di un pregiudizio in via generica e astratta, ma dovrà "… *b) valutare se il pregiudizio (concreto) prefigurato dipende direttamente dalla disclosure dell'informazione richiesta; c) valutare se il pregiudizio conseguente alla disclosure è un evento altamente probabile, e non soltanto possibile*"; tanto nel contesto temporale della domanda e privilegiando comunque la scelta più favorevole all'accesso. Nelle pagine successive si chiarisce ancora come il "pregiudizio concreto" (anche sul piano morale, sociale o relazionale) possa in tali casi consistere, ad esempio, in eventuali minacce, ritorsioni, azioni da parte di terzi, o furti di identità [44].

Se non andiamo errati, dunque, la regolazione formale del bilanciamento tra diritto al riserbo e diritto a conoscere induce logicamente e necessariamente a spostare l'asse della tutela del primo al livello dato dalla probabile produzione di quello che, con il linguaggio proprio dell'istituto aquiliano, chiameremmo un *danno conseguenza*, cioè un *quid pluris* rispetto al pregiudizio *in re ipsa* costituito dalla mera divulgazione dei dati personali. Il che significa ancora che, ponendoci nell'ottica di una controversia tra il cittadino i cui dati sono stati resi pubblici e la P.A. che vi ha dato accesso, il cittadino possa vedersi riconosciuto un diritto al risarcimento dei danni anche non patrimoniali solo se dà la prova di quel pregiudizio concreto, causalmente collegato all'ostensione del dato personale, in presenza del quale *soltanto* la norma sulla trasparenza consente il sacrifico del diritto di accesso [45].

Almeno su questo non secondario terreno, dunque, la mera violazione della norma a tutela dei dati personali non determina alcun pregiudizio risarcibile *in re ipsa* e immediatamente, se non corredata dalla dimostrazione di un danno *concreto* alla sfera personale dell'interessato. Sicché la dogmatica "difensiva" che assisterebbe in termini assoluti il diritto al controllo dei propri dati personali, a fronte della violazione della regola protettiva di condotta sembrerebbe cedere ad una dogmatica "relativizzata" dalla necessità formale di un bilanciamento tra valori costituzionali di pari grado. Circostanza che, con ogni evidenza, non può non trovare la sua ricaduta anche sul piano della tutela aquiliana, peraltro strumento non più esclusivo di protezione del diritto al controllo dei dati personali.

---

[44] Linee guida, cit. *supra*, pp. 11-19 ss. Resta evidente che le argomentazioni della P.A. destinataria della richiesta si formano nell'ambito di un procedimento rispettoso della disciplina di protezione dei dati, e perciò – fra l'altro – anche alla luce delle motivazioni (non vincolanti) addotte dal controinteressato.

[45] In tal senso, per tutti, E. CARLONI, M. FALCONE, *L'equilibrio necessario. Principi e modelli di bilanciamento tra trasparenza e privacy*, cit., p. 768 ss.

Ciò potrebbe essere ancor più vero se si riflette sul fatto che, imposto all'interessato un onere probatorio di un danno in concreto di fronte alla P.A. che divulga dati personali in ragione del principio di trasparenza della sua azione, non si vedrebbe come esonerare lo stesso interessato da analoga prova di fronte ad un titolare di trattamento privato la cui condotta posta in violazione della regola di riserbo non abbia prodotto un pregiudizio concreto e causalmente collegato alla violazione della regola, allorquando il titolare giustifichi il suo comportamento alla luce del principio di libertà di circolazione dei dati, direttamente invocando a bilanciamento il 3° comma dell'art. 1 del GDPR. Il che è quanto si cercava di argomentare nel punto precedente, e che adesso si vedrebbe rafforzato alla luce di un principio di parità di trattamento fra soggetti pubblici e soggetti privati che operano, ciascuno secondo le proprie regole e principi, attraverso la raccolta e l'elaborazione di dati personali.

Lo scenario che si è provato a tratteggiare vorrebbe rispecchiare la complessità nella quale la persona oggi si trova ad operare, a seguito sia dell'autorappresentazione di sé – probabilmente irreversibile – che i singoli mettono in campo attraverso l'uso delle risorse digitali, con conseguente esposizione del diritto al controllo dei propri dati alla continua interferenza con la libertà di circolazione vantata dai titolari del trattamento; sia dell'incorporazione dei dati personali nei processi produttivi e decisionali (oltre che delle imprese private, anche) delle pubbliche istituzioni, gravate del continuo e concreto bilanciamento tra gli obblighi di trasparenza e i doveri di rispetto della normativa a tutela dei dati personali.

Di qui, la necessità di una diversa precomprensione del conflitto tra riservatezza (in ogni senso) e circolazione delle informazioni e di una più flessibile misura del bilanciamento: in termini più chiari, una diversa misura di valutazione dell'illecito trattamento dei dati personali e del confine tra condotte invasive lecite e condotte invasive illecite. Il che, in fondo, altro non rappresenta che il normale svolgersi nel mondo del diritto dei criteri di valutazione del conflitto tra l'esigenza di conservazione di ciò che spetta a ciascuno e l'altrui libertà di azione, sullo sfondo dell'incentivazione dei comportamenti efficienti dei consociati idonei a massimizzare il benessere sociale condiviso [46].

6. – C'è infine un altro aspetto che ben si colloca in questo scenario. Ed è quello che si era accennato all'inizio con riferimento al fatto per cui l'offensività dell'economia basata sui dati rispetto alla persona si sviluppa in termini massivi e seriali, nel senso che

[46] Sempre utili e attuali perciò gli ammonimenti in tal senso di P. TRIMARCHI, *La responsabilità civile*, cit., pp. 43-44.

eventuali illeciti perpetrati dai giganti del digitale (ma non solo) colpiscono folle di danneggiati e serie indefinite di persone, peraltro nemmeno sempre catalogabili attraverso categorie predefinite. Potrebbero essere tutti i clienti di un certo servizio "social", come pure categorie di utenti/persone individuate in base alla razza o al sesso, o semplicemente in base al territorio geografico di residenza, o in base a qualunque altro criterio sviluppato nelle diverse tecniche di profilazione o di marketing, o nei procedimenti automatizzati utilizzati dalle pubbliche amministrazioni [47].

Mai come in questi casi lo strumentario della responsabilità aquiliana rivela la sua debolezza, o meglio la sua inefficienza rispetto al "danno" del quale vuol fornire un ristoro. La dimensione prettamente individualistica e volontaristica del rimedio aquiliano, a maggior ragione quando il danno da risarcire ha carattere non patrimoniale e dovesse richiedere – come si cercava di argomentare – anche la dimostrazione di un turbamento delle personali condizioni di benessere, rivela tutta la sua impotenza a fronte dell'azione offensiva realizzata in forma massiva da quei "regimi" o "sistemi normativi autonomi" che non hanno dimensione territoriale ma funzionale e dunque transnazionale, e sono in grado di imporre/proporre perciò un assetto di rapporti sociali strutturalmente dimensionato su larga scala e su numeri indefiniti. Forse i giuristi dovrebbero appropriarsi anche loro della conoscenza che altre discipline hanno sviluppato su ciò che, ad esempio, i quattro giganti del FAGA rappresentano sul piano politico, antropologico, oltre che ovviamente economico, e produrre soluzioni rimediali o di controllo adeguate.

Ed infatti, il consolidamento della dimensione globale e massiva del danno prodotto dall'azione di questi "sistemi" rende davvero ingenuo immaginare di reagire *solo* con gli strumenti della responsabilità aquiliana: seppur qualche individuo riuscisse ad ottenere ristoro personale delle lesioni subite, il danno sociale continuerebbe a persistere e a riprodursi in forma esponenziale, senza che le sofisticate teorie che presiedono all'applicazione dei rimedi aquiliani secondo i requisiti di fattispecie che un qualche giudice competente continuerebbe ad esigere (condotta illecita, lesione del diritto, causalità, danno risarcibile) siano minimamente in grado di creare un baluardo o quantomeno una deterrenza efficace.

---

[47] Ogni riferimento sul tema nei contributi citati in nota 15, cui adde G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Politica del diritto*, 2019, 2, p. 199 P. FEMIA, *Contrattazione algoritmica*, Relazione al 14° Convegno nazionale SISDIC su "Il trattamento algoritmico dei dati tra etica, diritto ed economia", Napoli maggio 2019, reperibile all'indirizzo *http://convegnisisdic.it/*; A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civili commentate*, 2017, 1, p. 144; S. CIVITARESE MATTEUCCI, *Umano troppo umano, decisioni amministrative automatizzate e principio di legalità*, in *Diritto pubblico*, 2019, 1, p. 6 F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alla predizioni dei* big data, *ibidem*, p. 43.

Ciò è quanto risulta dalle vicende giudiziarie che hanno (pressocché inutilmente) investito uno di quei giganti, Facebook, mettendo in difficoltà uno dei sistemi giurisdizionali più antichi e collaudati del mondo: l'Antitrust statunitense. La vicenda è nota e non la si vuole qui raccontare, se non per valorizzare il tentativo di colpire le massive e sistematiche violazioni dei diritti degli utenti al controllo dei propri dati personali non tanto attraverso la disciplina della privacy, quanto con gli strumenti dell'antitrust. A partire dalle prime indagini della *Federal trade commission* sulla condivisione non autorizzata di dati degli utenti da parte di terzi per fini commerciali e di marketing, infatti, si è fatta avanti l'idea che tutto ciò potesse rientrare nelle fattispecie tipicamente antitrust e fosse perciò perseguibile con i conseguenti strumenti: e così gli illeciti sulla privacy venivano riqualificati come abusi antitrust attraverso un collegamento tra i primi e l'esercizio (distorto) del potere di mercato da parte del *player*.

Mentre le dimensioni del problema prendevano la forma di *Cambridge Analytica*, tuttavia, la soluzione del problema si è costruita intorno agli strumenti degli accordi transattivi tra l'Autorità e il gigante del web e dell'irrogazione di sanzioni pecuniarie, nel dubbio teorico che quell'operazione di riqualificazione degli illeciti sulla privacy in chiave antitrust fosse legittima e opportuna.

Analoga vicenda si è svolta di recente in Germania, dove il dibattito sulla rilevanza delle modalità di raccolta dei dati personali in chiave di abuso e restrizione della concorrenza ha riportato in auge le più sofisticate discussioni teoriche sul concetto di "abuso" e sul nesso di causalità tra quest'ultimo e l'acquisizione di una posizione dominante di rilevanza per l'autorità antitrust [48].

In questa sede non interessa discutere né i passaggi interpretativi delle decisioni emanate e nemmeno gli esiti (spesso deludenti) che ne sono risultati.

Interessa solo argomentare come una corretta e appropriata impostazione dei rimedi contro l'offensività strutturale dell'economia digitale sulla persona non possa più sistemicamente essere regolata soltanto in chiave di responsabilità aquiliana, ma richieda l'utilizzazione di strumenti "altri" preventivi, di tipo macroeconomico se vogliamo, e non (soltanto) di diritto privato. E richieda soprattutto un autentico mutamento di cifra nella considerazione dei giganti del web, soggetti tutti privati, non più soltanto come tali, ma anche e soprattutto – indipendentemente dal loro status privatistico – come agenti di una funzione la cui invasività deve essere controllata con altri e più adeguati strumenti.

---

[48] Sulle interessantissime vicende qui indicate rinviamo ai contributi di C. OSTI, R. PARDOLESI, *L'antitrust ai tempi di Facebook*, in *Mercato concorrenza regole*, 2019, 2, p. 195 e A. GIANNACCARI, *Facebook, tra privacy e antitrust: una storia (non solamente) americana*, *ibidem*, p. 273.