APPUNTI SULLA RESPONSABILITÀ DA TRATTAMENTO DEI DATI*

NOTES ON DATA PROCESSING LIABILITY

Actualidad Jurídica Iberoamericana Nº 18, febrero 2023, ISSN: 2386-4567, pp. 1148-1171

* L'articolo costituisce il risultato delle ricerche condotte nell'ambito del progetto "TRUST- digital TuRn in EUrope: Strengthening relational reliance through Technology". *This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101007820. This article reflects only the author's view and the REA is not responsible for any use that may be made of the information it contains.*

Chiara IORIO

ARTICOLO CONSEGNATO: 12 de octubre de 2022
ARTICOLO APPROBATO: 5 de diciembre de 2022

ABSTRACT: Il presente contributo si propone di indagare alcune delle questioni più attuali in materia di circolazione dei dati personali. Premesso l'inquadramento della natura giuridica del dato, verrà esaminato il regime giuridico della responsabilità di cui all'art. 82 GDPR, con particolare riguardo alle ipotesi in cui l'illecito sia commesso dall'internet service provider, nonché nell'ambito di una Blockchain.

PAROLE CHIAVE: Dati personali; trattamento illecito; responsabilità; risarcimento del danno; internet service provider; Blockchain.

ABSTRACT: *This paper focuses on some of the most controversial issues concerning the circulation of personal data. The legal nature of personal data will be framed. Then, the liability regime pursuant to Article 82 GDPR will be examined, with particular reference to data breach committed by an Internet service provider and in the context of a Blockchain.*

KEY WORDS: *Data protection; data breach; liability; damages; internet service provider; Blockchain.*

SOMMARIO.- I. PREMESSA – II. LA NATURA DEL DATO PERSONALE, TRA DIRITTO FONDAMENTALE E BENE COMMERCIABILE – III. LA RESPONSABILITÀ PER ILLECITO TRATTAMENTO DEI DATI – IV. LA RESPONSABILITÀ DELL'INTERNET SERVICE PROVIDER PER ILLECITO TRATTAMENTO DEI DATI – V. ILLECITO TRATTAMENTO DATI E BLOCKCHAIN. – 1. I principi di minimizzazione e data protection by design – 2. La identificazione del titolare e del responsabile del trattamento – VI. CONSIDERAZIONI CONCLUSIVE.

I. PREMESSA.

L'innovazione digitale e la connessa dematerializzazione della realtà hanno attribuito una rilevanza centrale ai dati personali, tanto che da più parti si discute di una oramai compiuta "datificazione"[1], ovvero, con accenti meno neutri, di "datacrazia"[2].

Il "dato" acquista, invero, una dimensione polivalente, in cui il confine tra pubblico e privato si fa meno netto[3]: da attributo della persona, esso diviene motore del progresso tecnologico[4], mezzo di controllo dei titolari[5] e, quindi, strumento per l'esercizio del potere da parte dello Stato[6].

Non è un caso che, a livello euro-unitario, anche nel recente Pacchetto sui "Servizi digitali" la protezione degli utenti online e lo stimolo all'innovazione abbiano richiesto una attenta regolamentazione dell'impiego e della circolazione dei dati.

Se, dunque, la disciplina a riguardo non ha ancora raggiunto un assetto definitivo, i problemi emergenti nella realtà esigono risposte immediate dal giurista.

1 Così, Calzolaio, S.: "Protezione dei dati personali" (voce), *Dig. disc. pubbl*., 2017, p. 594.

2 Cfr. voce "Datacrazia", in www.treccani.it.

3 Autorevole dottrina già da tempo auspica il superamento della dicotomia tra pubblico e privato. Cfr. Perlingieri, P: "L'incidenza dell'interesse pubblico sulla negoziazione privata", *Rass. dir. civ*., 1986, 4, p. 57.

4 Come noto, invero, i dati personali alimentano le tecnologie in grado di apprendere dall'esperienza, quali quelle di "machine learning" e "deep learning": Cfr: D'Acquisto, G.: "Intelligenza artificiale", in *I diritti nella "rete" della rete. Il caso del diritto d'autore"* (dir. da F. Pizzetti), Giappichelli, Torino, 2021, p. 127.

5 Si pensi agli strumenti di controllo sociale sperimentati in Cina, dove la commistione della tecnologia nella vita privata fa il paio con l'ingerenza penetrante dello Stato nelle esistenze individuali, con la conseguenza che il potere pubblico è legittimato ad ottenere dai provider i dati personali di qualsivoglia utente, laddove generiche ragioni di sicurezza lo rendano necessario. In arg. Soro, A.: "La protezione dei dati personali nell'era digitale", *Nuova giur. civ. comm*., 2019, 2, p. 343. Cfr., anche Sciascia, G.: "Reputazione e potere: il social scoring tra distopia e realtà", *Giorn. dir. amm*., 2021, 3, p. 317.

6 Calzolaio, S.: "Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati", *Riv. it. inf. e dir*., 2021, p. 7, ove l'A. afferma che l'avvento delle nuove tecnologie ha introdotto "un collegamento strutturale, e non temporaneo, fra disponibilità dei dati da parte degli Stati e imperium, cioè capacità di esercizio del potere sovrano. Con espressione sintetica: ubi data, ibi imperium".

• Chiara Iorio
Assegnista di ricerca, Università degli Studi di Macerata
c.iorio@unimc.it

Il presente contributo si propone di esaminare alcune delle questioni più controverse e attuali in materia. Prendendo le mosse dall'inquadramento della natura e delle modalità di circolazione dei dati, sarà indagato il regime di responsabilità di cui all'art. 82 GDPR, con particolare riguardo all'illecito commesso dall'internet service provider, o nell'ambito di una Blockchain.

II. LA NATURA DEL DATO PERSONALE, TRA DIRITTO FONDAMENTALE E BENE COMMERCIABILE.

La pluralità di interventi regolatori che, negli ultimi anni, ha interessato la disciplina dei dati personali conferma la centralità che questi ultimi hanno assunto nell'attuale società tecnologica, e ne pone in luce molteplici criticità sul piano giuridico.

La necessità di un approccio disciplinare differenziato in materia discende dalla ambivalente natura del dato personale, conteso tra la logica mercantilistica, che ne vorrebbe l'equiparazione ad un bene, e quella personalistica, che lo erige a diritto fondamentale. La prima impostazione (la "mercantilistica") appare aderente alla realtà economica, nella quale è frequente la cessione dei dati personali in cambio della fruizione di servizi digitali[7]. La seconda (la "personalistica"), più tradizionale, si fonda sulla espressa inclusione della protezione dei dati di carattere personale tra i diritti fondamentali, di cui all'art. 8 Carta UE. Secondo questa prospettiva, i dati non potrebbero circolare come ricchezza, ma sarebbero un attributo della persona, fondamento di una nuova concezione del diritto alla "privacy"[8]. Una posizione soggettiva, quest'ultima, da non confinare più nella accezione "negativa" della riservatezza[9] rivendicata dal singolo rispetto a invasioni della sfera privata (specialmente nel contesto delle attività di cronaca), ma da intendersi nel senso (positivo) del diritto, da parte di ciascuno, di esercitare un controllo effettivo sui dati immessi in rete[10].

7 Insiste sul punto Ricciuto, V.: "Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali", *Riv. dir. civ.*, 2020, 3, p. 642; in arg., si rinvia anche a De Franceschi, A.: *La circolazione dei dati personali tra privacy e contratto*, Napoli, Esi, 2017, p. 10, e, con specifico riferimento all'adesione ad un social network tramite consenso al trattamento di dati personali dell'utente, Perlingieri, C.: *Profili civilistici dei social networks,* Napoli, Esi, 2014, p. 80.

8 Sulla evoluzione del diritto alla *privacy* si rinvia a Cuffaro, V.: "Il diritto europeo sul trattamento dei dati personali", *Contr. impr.*, 2018, 3, p. 1098; Visintini, G: "Dal diritto alla riservatezza alla protezione dei dati personali", *Dir. inf.* e *informatica*, 2019, p. 1.

9 Su cui si vedano le risalenti indagini di Giampiccolo, G.: "La tutela giuridica della persona umana e il c.d. diritto alla riservatezza", *Riv. trim. dir.* e *proc. civ.*, 1958, p. 458; Rescigno, P.: "*Il diritto all'intimità della vita privata*", in *Studi in onore di F. Santoro-Passarelli*, IV, Jovene, Napoli, 1972, p. 121; Pugliese, G.: "Il diritto alla riservatezza nel quadro dei diritti della personalità", *Riv. dir. civ.*, 1963, p. 605.

10 In arg., Rodotà, S.: "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", *Riv. crit. dir. priv.*, 1997, p. 583; Finocchiaro, G.: "Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali", in *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 ago- sto 2018, n. 101*, (a cura di G. Finocchiaro), Zanichelli, Bologna, 2019, p. 5.

Della tensione tra le due opposte visioni circa la natura del dato vi è traccia nello stesso iter legislativo della Direttiva 770/2019, in tema di contratti di fornitura di contenuto digitale e di servizi digitali[11]. Nel testo della proposta, invero, il conferimento dell'accesso ai dati personali, da parte di un consumatore, era espressamente qualificato come "controprestazione non pecuniaria" rispetto alla fruizione di un contenuto digitale. La formulazione definitiva della direttiva – accogliendo i rilievi mossi dal Garante europeo per la protezione dei dati[12] – rigetta l'equiparazione tra dati personali e merce[13] ed espunge formalmente l'accesso a contenuti digitali tramite cessione dei dati personali dall'ambito dei contratti corrispettivi. L'art. 3, infatti, distingue l'ipotesi in cui l'operatore economico offra contenuti digitali contro corresponsione del prezzo, da quella in cui il consumatore si impegni a fornire, in cambio, dati personali. Pur applicandosi la direttiva ad entrambe le fattispecie, la prima è qualificata espressamente come "contratto", mentre la seconda è denominata genericamente come "caso".

E tuttavia, al di là della – pur discutibile – formulazione letterale, non pare che le due vicende siano diversamente disciplinate, sul piano sostanziale. La direttiva, invero, estende anche alla fornitura di servizi digitali senza corrispettivo in denaro l'applicazione dei rimedi contro i difetti di conformità, sicché, nei fatti, la vicenda apparentemente gratuita è equiparata, sul piano disciplinare, a quella onerosa.

Nello stesso senso, anche la dir. 2161/2019[14], che, al considerando n. 31, avverte la "somiglianza" e la "interscambiabilità" tra servizi digitali erogati contro il pagamento di un prezzo e quelli forniti nel contesto dell'accesso ai dati personali, sì da prospettare l'estensione ai secondi delle tutele previste, in base al diritto dei consumatori, per le prime. In tale direzione, ancora, il nuovo art. 3-*bis* della dir. UE 2011/83[15], che sancisce l'applicazione della direttiva anche alle ipotesi di fornitura di servizi, da parte del professionista, contro l'accesso ai dati, da parte del consumatore.

11 Per un'attenta analisi della direttiva si rinvia a Camardi, C.: "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", *Giust. civ.*, 2019, p. 499.

12 Cfr. Parere del Garante europeo per la protezione dei dati reso il 17 marzo 2017 (EDPS, Opinion 4/2017, in www. edps.europa.eu), dove si afferma che "i diritti fondamentali, come il diritto alla protezione dei dati personali, non possono essere ridotti a semplici interessi dei consumatori e i dati personali non possono essere considerati una mera merce".

13 Il considerando n. 24 recita: "la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce".

14 Dir. UE 2019/2161 del Parlamento Europeo e del Consiglio del 27 novembre 2019 che modifica la dir. 93/13/CEE del Consiglio e le dir. 98/6/CE, 2005/29/CE e 2011/ 83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori.

15 Dir. UE 2011/83 del Parlamento Europeo e del Consiglio del 25 ottobre 2011sui diritti dei consumatori, recante modifica della direttiva 93/13/CEE del Consiglio e della direttiva 1999/44/CE del Parlamento europeo e del Consiglio e che abroga la direttiva 85/577/CEE del Consiglio e la direttiva 97/7/CE del Parlamento europeo e del Consiglio.

Tali soluzioni appaiono condivisibili sul piano della teoria generale, e risultano coerenti con l'effettiva dinamica dei traffici in rete.

Se, infatti, appare innegabile la collocazione della protezione dei dati personali nell'ambito dei diritti della personalità, non può, nondimeno, escludersi che il consenso al loro trattamento, quale condizione per la fruizione di servizi digitali, inneschi una vicenda negoziale caratterizzata da corrispettività. Più in particolare, come condivisibilmente osservato, in tali eventualità il trattamento dei dati diviene elemento di una fattispecie contrattuale complessa, nella quale figura una duplice manifestazione di consenso: quello alla fruizione del servizio digitale, in assenza della corresponsione di un prezzo in denaro, da un lato; quello all'accesso ai propri dati, dall'altro.

È evidente che i due atti di "consenso"[16] non possano essere studiati autonomamente, ma siano collegati, sul piano funzionale della "causa concreta", nel senso che l'assenso al trattamento si giustifica proprio in ragione della fornitura del servizio, di cui costituisce, in altri termini, il corrispettivo[17].

Se, dunque, la fattispecie in esame può dar vita ad un contratto di scambio a titolo oneroso[18], va escluso che si configuri una compravendita, come pure affermato in un'occasione dalla giurisprudenza[19]. Proprio la peculiarità del dato

16 Sulla natura del consenso al trattamento dei dati non v'è uniformità di vedute in dottrina. Alcuni lo considerano come consenso negoziale (cfr. Oppo, G.: "«Trattamento» dei dati personali e consenso dell'interessato", in Id., *Scritti giuridici*, VI, *Principi e problemi del diritto privato*, CEDAM, Padova, 2000, p. 113; Cuffaro, V.: "A proposito del ruolo del consenso", in *Trattamento dei dati e tutela della persona* (a cura di V. Cuffaro, V. Ricciuto, V. Zeno Zencovich,) Giuffré, Milano, 1999, p. 121) altri lo qualificano come atto giuridico in senso stretto, nei termini di scriminante (Patti, S.: "Il consenso dell'interessato al trattamento dei dati personali", *Riv. dir. civ.*, 1999, p. 455) ovvero di atto meramente autorizzatorio (Bravo, F.: "Lo «scambio di dati personali» nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto", *Contr. e impr.*, 2019, p. 34; Messinetti, R.: "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali", *Riv. crit. dir. priv.*, 1998, p. 35). In arg., Solinas, C.: "Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette", *Giur. it.*, 2021, p. 325.

17 Cfr. Ricciuto, V., *op. cit.*, p. 652, per il quale "la funzione economica, insomma, è quella di realizzare, concretamente ed al di là degli schemi utilizzati, uno scambio, anche laddove lo schema contrattuale sia apparentemente gratuito". Di diverso segno è l'impostazione di Camardi, C., *op. cit.*, p. 550, per la quale l'operazione negoziale sarebbe ricostruibile nei termini di una fornitura di beni/servizi digitali "a struttura gratuita", cui si affianca, ma non in funzione corrispettiva, un atto dispositivo con cui il consumatore cede i dati personali, a scopo non commerciale.
In giurisprudenza, cfr. la sentenza del Consiglio di Stato, 29 marzo 2021, n. 2631, in *GiustiziaCivile.com*, con nota di Ricciuto, V. e Solinas, C.: "Fornitura di servizi digitali e prestazione di dati personali: punti fermi ed ambiguità sulla corrispettività del contratto". Nella sentenza si legge che i servizi del social network Facebook sono "promessi come gratuiti, ma che, evidentemente, gratuiti non sono, finendo per rappresentate il «corrispettivo» della messa a disposizione dei dati personali del singolo utente a fini commerciali".

18 Tale soluzione, con specifico riferimento all'accordo tra social network e utente, è sostenuta anche da Peringieri, C.: *op. cit.*, p. 88. L'A. osserva che "la disposizione della privacy e dei dati personali è in funzione dell'utilizzo della piattaforma, sì che in virtù del sinallagma, l'utente ha tanto il diritto di utilizzare la piattaforma – e il social è obbligato a consentirne l'utilizzo – in quanto il social può raccogliere e sfruttare dati personali. In senso adesivo rispetto alla natura del contratto di scambio a titolo oneroso, anche De Franceschi, A.: *La circolazione dei dati personali tra privacy e contratto*, cit., p. 75.

19 Cfr. Tar Lazio, 10 gennaio 2020, n. 260, in *Giur. it.*, 2021, p. 320, con nota di Solinas, C.: "Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette", cit.

personale (che attiene ad un diritto fondamentale) conduce a negare che lo stesso possa essere ceduto in via definitiva ad altri. Si rammenti, peraltro, che, ai sensi dell'art. 7, par. 3, GDPR, il titolare del dato ha, in "qualsiasi momento", il diritto di revocare il proprio consenso. Ad essere ceduto è, più precisamente, il diritto di sfruttamento economico del dato, mediante uno schema che, secondo alcuni, sarebbe qualificabile in termini di "licenza"[20].

Peraltro, va rilevato che la negazione della natura "anche" commerciale dei dati si traduce, sul piano applicativo, in una tutela mutilata per il titolare. In assenza di puntuali disposizioni normative (ulteriori rispetto alle direttive citate), invero, la concezione personalistica dovrebbe condurre a ritenere applicabile, sul piano delle tutele, i soli rimedi previsti per i diritti della personalità e quelli di cui al GDPR. Dovrebbe, viceversa, escludersi che il titolare possa avvalersi della disciplina dei fenomeni patrimoniali, tra cui, anzitutto, quella prevista in tema di pratiche commerciali scorrette.

Viceversa, ammettendo che i dati personali, pur riguardando la personalità dell'individuo, possano circolare anche a fini commerciali, non potrebbe escludersi l'integrale applicazione della disciplina consumeristica. Così, nelle ipotesi – frequentissime – in cui l'operatore professionale non informi il consumatore – il quale sia, quindi, convinto della gratuità del servizio – della profilazione dei suoi dati a fini commerciali, potrà risultare configurabile una pratica commerciale scorretta, *ex* artt. 20, 21 e 22 Cod. cons., e/o aggressiva, ai sensi degli artt. 20, 24 e 25 Cod. cons.

In tal modo, si supera la logica dei "compartimenti stagni di tutela", in favore di una concezione di "tutela multilivello" [21] in grado di assicurare una protezione effettiva dei diritti delle persone fisiche, nell'ipotesi in cui un diritto personalissimo sia sfruttato a fini commerciali, anche indipendentemente dalla volontà dell'interessato.

20 Zeno-Zencovich, V.: "Do "Data Markets" Exist?", *MediaLaws*, 2019, p. 26. Sul punto, cfr. anche Ricciuto, V., "Il contratto ed i nuovi fenomeni patrimoniali", cit., p. 656, per il quale "i diritti ipotizzabili sugli stessi che vengono trasmessi o acquisiti dal titolare del trattamento possono essere di diverso tipo, di godimento non esclusivo, di sfruttamento economico, di trasformazione al fine della creazione di ulteriori dati attraverso, ad esempio, la profilazione, ecc".

21 Di "tutele multilivelli" discorre Consiglio di Stato, 29 marzo 2021, n. 2631, cit., il quale rigetta la tesi per la quale dovrebbe ritenersi applicabile – in ragione della sua pretesa specialità – la sola normativa del GDPR, con l'effetto di escludere l'applicabilità di ogni altra disciplina giuridica. Ferma la centralità del GDPR, il Consiglio di Stato esclude che, in materia, si possano ravvisare "compartimenti stagni di tutela". Ne consegue che, "allorquando il trattamento investa e coinvolga comportamenti e situazioni disciplinate da altre fonti giuridiche a tutela di altri valori e interessi (altrettanto rilevanti quanto la tutela del dato riferibile alla persona fisica), l'ordinamento - unionale prima e interno poi - non può permettere che alcuna espropriazione applicativa di altre discipline di settore (…) riduca le tutele garantite alle persone fisiche".

III. LA RESPONSABILITÀ PER ILLECITO TRATTAMENTO DEI DATI.

Altrettanto controversa appare la ricostruzione del regime di responsabilità derivante dal trattamento dei dati, attualmente disciplinato dall'art. 82 GDPR.

Il dibattito ripropone in veste nuova le argomentazioni che già avevano animato la dottrina nel vigore del vecchio Codice privacy. Come noto, invero, il richiamo, da parte dell'art. 15 del D. Lgs. 196/2003[22], all'art. 2050 c.c. era stato variamente interpretato dagli studiosi. Stando all'impostazione maggioritaria, si sarebbe trattato di una fattispecie di responsabilità aquiliana, secondo alcuni generalmente riconducibile al paradigma di cui all'art. 2043[23], da altri studiata come responsabilità speciale[24]. Restavano minoritarie le opinioni che, interpretando la menzione dell'art. 2050 nei sensi del rinvio alla sola regola probatoria ivi prevista, riconducevano la fattispecie all'ambito contrattuale[25].

Gli interrogativi si ripropongono alla luce del testo del Regolamento che, mediando tra le diverse culture giuridiche dei Paesi membri[26], prevede all'art. 82 il diritto, in capo a "chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento", di "ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".

Nonostante la formulazione letterale della disposizione possa richiamare alla mente l'art. 2043 del nostro Codice civile, un'analisi più attenta svela l'inadeguatezza di una ricostruzione in chiave unitaria della responsabilità[27].

Può distinguersi, anzitutto, il regime di responsabilità del titolare da quello del responsabile del trattamento. Il secondo comma dell'art. 82, invero, grava il titolare

22 L'art. 15 Cod. privacy prevedeva che "Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.".

23 Stando a questa interpretazione, in particolare, la fonte della responsabilità sarebbe pur sempre un danno ingiusto (dove la meritevolezza della situazione giuridica soggettiva lesa andrebbe valutata caso per caso) cagionato da una condotta *contra ius* dolosa, ovvero colposa. Cfr. Caringella, F.: "La tutela aquiliana della privacy nel codice per la protezione dei dati personali (d. lgs. n. 196/2003), in Id., *Studi di diritto civile*. III. *Obbligazioni e responsabilità*, Giuffré, Milano, 2005, p. 715.

24 Roppo, V.: "La responsabilità civile per trattamento di dati personali", *Danno resp.*, 1997, p. 663.

25 Scognamiglio, C: "Buona fede e responsabilità civile", *Eur. dir. priv.*, 2001, p. 357; Busnelli, F. D.: "Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte", *Contr. impr.*, 1991, p. 539; Castronovo, C: "Situazioni soggettive e tutela nella legge sul trattamento dei dati personali", *Eur. dir. priv.*, 1998, p. 656; Pellecchia, E.: "La responsabilità civile per trattamento dei dati personali", *Resp. civ. prev.*, 2006, p. 221.

26 Sul punto, sottolinea che, nel vigore della esistente regolamentazione, le categorie giuridiche domestiche devono cedere il passo a quelle europee, nelle dinamiche del "droit pluriel" Bravo, F.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi Galgano), Wolters Kluver, Milano, 2019, p. 393.

27 Tra le prime interpretazioni dell'art. 82 GDPR, è diffusa, tuttavia, la qualificazione della responsabilità da trattamento dei dati come extracontrattuale. *Ex multis*, cfr. Gambini, M.: *Principio di responsabilità e tutela aquiliana dei dati personali,* Esi, Napoli, 2018, spec. p. 124; Tosi, E.: *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Giuffré, Milano, 2019, p. 49.

del risarcimento del danno "cagionato dal suo trattamento che violi il presente regolamento"; quindi, chiama a rispondere il responsabile nella duplice eventualità in cui costui a) non abbia "adempiuto gli obblighi del presente regolamento specificatamente diretti" a lui stesso, ovvero b) abbia "agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento".

Si ritiene di poter affermare che, mentre il titolare sarà tenuto a rispondere sempre a titolo contrattuale, il responsabile del trattamento sarà soggetto a responsabilità da inadempimento nella sola ipotesi sub a). Al fine di comprendere tale assunto, appare imprescindibile chiarire il radicale mutamento dell'impianto – e, dunque, dei relativi principi fondativi – su cui è strutturato il regolamento, rispetto alla "vecchia" dir. 95/46/CE[28].

La più recente disciplina, invero, grava il titolare e il responsabile del trattamento di una serie di obblighi di comportamento specifici[29], volti ad assicurare la liceità del trattamento e, dunque, il rispetto dei diritti del titolare del dato (di cui all'art. 5 GDPR): è, così, data attuazione al principio della "responsabilizzazione" (c.d. "accountability"), che, privilegiando un approccio ex ante, è funzionale a prevenire il rischio di verificazione di danni[30].

Al contempo, tale mutamento di prospettiva, esigendo dai menzionati soggetti l'adempimento di puntuali obblighi legali, colloca il rapporto tra costoro e il titolare del dato in una dinamica di tipo relazionale[31]. Ne consegue che, laddove in capo al titolare del dato residui un danno, per effetto "della violazione del regolamento" (art. 82), sarà ravvisabile una ipotesi di responsabilità da inadempimento, ex art. 1218 c.c.

Tale soluzione appare facilmente argomentabile nel caso in cui i soggetti siano già parte di un rapporto negoziale, laddove il trattamento sia necessario "all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso" (art. 6, comma 1, lett. b). A identiche conclusioni dovrà giungersi anche nei casi in cui l'interessato presti un

28 Per un commento della relativa disciplina, si rinvia a Bianca, C. M. -Busnelli, F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 (« Codice della privacy »)*, I, Cedam, Padova, 2009; Cuffaro, V. -D'Orazio, G. -Ricciuto, V. (a cura di): *Il Codice del trattamento dei dati personali*, Giappichelli, Torino, 2007; Sica, S. – Stanzione, P. (a cura di): *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Zanichelli, Bologna, 2005.

29 Si pensi, *ex multis*, agli obblighi aventi ad oggetto l'adozione di misure di sicurezza, di cui agli artt. 24, 25 e 32; agli obblighi derivanti dalla applicazione dei diritti dell'interessato, di cui agli artt. 12-22; alle disposizioni relative al consenso informato, di cui agli artt. 6, par. 1 lett. a) e 9, par. 1, lett. b).

30 Cfr., sul punto, Renna, M.: "Sicurezza e gestione del rischio nel trattamento dei dati personali", *Resp. civ. prev.*, 2020, p. 1343.

31 Cfr. Piraino, F.: "Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civ. comm.*, 2017, p. 369; nello stesso senso anche Zecchin, F.: "Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali", *Eur. e dir. priv.*, 2022, p. 517.

consenso specifico al trattamento dei dati, ovvero nelle altre ipotesi in cui l'art. 6 riconosca l'esistenza di una legittima base giuridica per il trattamento: il complesso di obblighi informativi (artt. 12, 13, 14) e di sicurezza (art. 32) che, anche in tali eventualità, gravano sul titolare (e, in taluni casi, sul responsabile) fanno sì che questi ultimi non possano essere considerati come un "passante"[32], onerato di un generico dovere di "neminem laedere". La fattispecie di cui all'art. 2043 c.c., invero, presuppone che il rapporto tra danneggiante e danneggiato origini con il danno, mentre, nel caso che ci occupa, è ravvisabile un obbligo preesistente alla verificazione del pregiudizio in capo al titolare del dato. Le disposizioni del GDPR, dunque, codificano obbligazioni *ex lege* (da ricomprendersi nelle "variae causarum figurae" di cui all'art. 1173 c.c.) e sono idonee a fondare, se inosservate, una classica ipotesi di responsabilità da inadempimento.

Sembra, allora, che potrà ravvisarsi una responsabilità aquiliana nelle due sole ipotesi, del tutto residuali in cui: a) il responsabile del trattamento abbia agito "in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento", posto che, in tale eventualità, non si ravvisa un rapporto giuridico tra responsabile e interessato[33]; b) il trattamento dei dati avvenga, da parte di un soggetto non qualificabile come titolare né responsabile del trattamento[34], al di fuori dell'esistenza di una legittima base, di cui all'art. 6 GDPR.

Sul piano disciplinare, l'art. 82 esonera il titolare o il responsabile dalla responsabilità, previa dimostrazione, da parte di costui, "che l'evento dannoso non gli è in alcun modo imputabile". Tale formulazione – che ricalca il tenore dell'art. 1218 c.c. – implica una presunzione dell'esistenza del nesso causale, sicché, una volta dimostrata la sussistenza del danno e allegato l'inadempimento (ovvero, se si configura una responsabilità aquiliana, dimostrato il fatto illecito), da parte dell'interessato, si innesca una inversione dell'onere probatorio, a suo vantaggio.

Va, infine, precisato che le summenzionate obbligazioni di condotta previste dal regolamento hanno una natura prettamente procedimentale[35] e non attribuiscono, pertanto, una immediata utilità al titolare. Ne consegue che la condanna al risarcimento del danno presuppone, in ogni caso, la prova di un danno "materiale o immateriale" effettivamente residuato in capo all'interessato. Nell'ipotesi, invece, in cui risulti configurabile una responsabilità aquiliana, il risarcimento è subordinato

32 La teorizzazione della responsabilità aquiliana come responsabilità del passante si deve a Carlo Castronovo. Cfr, da ultimo, Id, *Responsabilità civile*, Giuffré, Milano, 2018, p. 551.

33 Il responsabile, invero, è soggetto a responsabilità (ai sensi del secondo comma dell'art. 82 GDPR) nel caso in cui "non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento" o se "ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento". Cfr. Bravo, R.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", cit., p. 383.

34 Tale qualifica, invero, innesca la serie di obblighi di condotta che inducono ad affermare l'esistenza di un rapporto obbligatorio.

35 Cfr. Piraino, F.: "Il regolamento generale sulla protezione dei dati personali", cit., p. 390.

alla prova dell'ingiustizia del danno, posto che, in accordo alla teoria generale della responsabilità civile, devono escludersi ipotesi di ingiustizia "in re ipsa"[36].

IV. LA RESPONSABILITÀ DELL'INTERNET SERVICE PROVIDER PER ILLECITO TRATTAMENTO DEI DATI.

Assai delicato è l'accertamento della responsabilità nel caso in cui l'illecito trattamento dei dati sia avvenuto nel contesto della prestazione di un servizio della società dell'informazione. Posto che il GDPR (art. 2, comma 4) fa espressamente salva l'applicazione della direttiva 2000/31/CE, con particolare riguardo alle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15, s'impone la necessità di un coordinamento tra le due discipline.

Come noto, la direttiva c.d. "e-commerce" ha delineato un regime speciale di responsabilità per i provider, informato all'obiettivo di fornire impulso al mercato digitale[37]. Tale disegno si è tradotto nella previsione di plurime cause di esclusione della responsabilità dei prestatori, a seconda dell'attività espletata[38]. Non sono neppure introdotti generalizzati obblighi di condotta in capo al provider[39].

36 In tal senso, peraltro, anche la giurisprudenza nel vigore del Codice privacy, che affermava di frequente che "il danno non patrimoniale risarcibile [...] non si sottrae alla verifica della "gravità della lesione" e della "serietà del danno" [...] sicché determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni [...] ma solo quella che ne offenda in modo sensibile la sua portata": così Cass. 8 febbraio 2017 n. 3311, in *DeJure*; nello stesso senso anche Cass. 5 settembre 2014 n. 18812, *ivi*; Cass. 15 luglio 2014 n. 16133, *ivi*. Ma in favore della natura in re ipsa del danno ingiusto, si veda Tosi, E., *op. cit*., p. 240.

37 Appare opportuno precisare che il recentissimo Digital Services Act [Reg. (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali)], che troverà applicazione a decorrere dal 17 febbraio 2024, disciplina la responsabilità dei provider in senso sostanzialmente analogo alla "vecchia" direttiva "e-commerce". Si mantiene, nel dettaglio, la previsione delle cause di esenzione della responsabilità, distinguendo tra prestatori di servizio di "mero trasporto" (art. 4), "memorizzazione temporanea" (art. 5) e "hosting" (art. 6). Sostanziali innovazioni consistono nella introduzione, all'art. 6, di una causa di esclusione del beneficio dell'esenzione di responsabilità; nella previsione, all'art. 7, della clausola del c.d. "buon samaritano", e nella introduzione di obblighi specifici di azione, in capo al provider, nel caso di contenuto illecito (artt. 9 e 10).

38 Vanno esenti da responsabilità, anzitutto, gli intermediari che si limitino ad un'attività di "mere conduit", vale a dire di semplice trasporto (art. 12 dir; art. 14 D. Lgs. 70/2003), e quelli che realizzino una memorizzazione temporanea (c.d. "catching"), sempre che non modifichino le informazioni trasmesse e, se edotti di una irregolarità in piattaforma, agiscano prontamente per rimuovere le informazioni memorizzate, o per disabilitare l'accesso (art. 13; art. 15. D. lgs 70/2003). Anche la memorizzazione permanente (c.d. "hosting") non comporta la responsabilità del gestore, sempre che quest'ultimo non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e che, non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso (art. 14 direttiva; art. 16 D. Lgs. 70/2003).

39 Nell'ottica di chiusura del sistema, è altresì esclusa la soggezione dei prestatori ad obblighi di sorveglianza sulle informazioni trasmesse, di memorizzazione, ovvero di ricerca attiva di fatti o circostanze indicative di condotte illecite (art. 15 direttiva; art. 17 D.lgs. 70/03513). Soltanto laddove il prestatore venga a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione scatta l'obbligo di informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza (così, art. 17, comma 2, lett a). Il terzo comma del medesimo articolo precisa che "Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente".

Si rammenti, tuttavia, che, constatata l'inadeguatezza di un sì fatto regime di sostanziale immunità[40] a fronte del massiccio sviluppo delle relazioni digitali, la giurisprudenza – in primis comunitaria – ha operato una tendenziale riconduzione della responsabilità in parola entro il sistema ordinario di responsabilità. Ne è derivata la distinzione tra provider "passivo"[41] – cui le ipotesi di esenzione trovano integrale applicazione – e "attivo", responsabile ai sensi del regime generale di cui all'art. 2043 c.c[42]. Tale distinzione corrisponde a quella – tradizionale – della condotta illecita che, come noto, "può consistere in un'azione o in un'omissione, in tale ultimo caso con illecito omissivo in senso proprio, in mancanza dell'evento, oppure, qualora ne derivi un evento, in senso improprio; a sua volta, ove l'evento sia costituito dal fatto illecito altrui, si configura l'illecito commissivo mediante omissione in concorso con l'autore principale"[43]. La figura del provider attivo va, allora, generalmente ricondotta alla fattispecie della condotta illecita attiva di concorso.

40 Non a caso Bocchini, F.: "Responsabilità dell'hosting provider, la responsabilità di Facebook per la mancata rimozione di contenuti illeciti", *Giur. it*., 2017, p. 629, definisce la Dir. 2000/31/CE come "la direttiva dell'irresponsabilità".

41 Invero, la Corte di Giustizia è giunta a limitare l'applicazione del regime speciale ex art. 14 dir. ai soli casi in cui il ruolo svolto dal gestore sia "neutro". Si richiede, a tal fine, che la condotta sia meramente tecnica, automatica e passiva, ciò che implica mancanza di conoscenza o di controllo dei contenuti memorizzati: Corte giust. UE 23 marzo 2010, (causa C-236/08, Google c. Louis Vuitton), in *Dir. inf*., 2010, p. 49; Corte giust. UE 12 luglio 2011 (causa C-324/09, L'Oreal c. e-Bay), cit. Vedi anche Corte giust. UE 14 giugno 2017 (causa C-610), in *Diritto, mercato e tecnologia*, 2018, con nota di Scuderi, S.: "La responsabilità dell'internet service provider alla luce della giurisprudenza della Corte di Giustizia Europea". La distinzione tra hosting provider passivo e attivo è stata recepita immediatamente dalla giurisprudenza nazionale, che applica solo al primo il regime di esonero di cui all'art. 16, mentre sottopone al giudizio ordinario di ex art. 2043 il gestore ("attivo") che "svolge un'attività che esula da un servizio di ordine meramente tecnico, automatico e passivo, e pone, invece, in essere una condotta attiva, concorrendo con altri nella commissione dell'illecito. Cass., 19.3.2019, n. 7708, in *Foro it*., 2019, I, c. 2045; in argomento, Di Ciommo, F.: "Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea", *Foro it*., 2019, I, p. 2078; Cassano, G.: "La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider", *Dir. ind*., 2019, 4, p. 35; Bocchini, F.: "La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP", *Giur.it*., 2019, p. 2604; Gambini, M. L.: "La responsabilità dell'internet service provider approda in Cassazione", *Corr. giur.,* 2020, 2, p. 177. Più in particolare, la giurisprudenza di merito ha enucleato talune figure sintomatiche idonee a rilevare il carattere attivo della prestazione. Si considerino, a titolo esemplificativo, quelle di "filtro, selezione, indicizzazione, organizzazione, catalogazione, aggregazione, valutazione, uso, modifica, estrazione o promozione dei contenuti, operate mediante una gestione imprenditoriale del servizio, come pure l'adozione di una tecnica di valutazione comportamentale degli utenti per aumentarne la fidelizzazione: condotte che abbiano, in sostanza, l'effetto di completare ed arricchire in modo non passivo la fruizione dei contenuti da parte di utenti indeterminati". In tali casi, dunque, l'affermazione della responsabilità dell'intermediario è subordinata all'accertamento degli elementi costitutivi della fattispecie di cui all'art. 2043 c.c.

42 Il regime di immunità viene meno, dunque, nel caso in cui il provider svolga un ruolo attivo, idoneo a conferirgli una conoscenza o un controllo dei suddetti contenuti. Appare, quindi, imprescindibile che il "carattere illecito dell'attività o dell'informazione debba risultare da una conoscenza effettiva o essere manifesto, vale a dire che esso deve essere concretamente dimostrato o facilmente identificabile" (così, Corte di Giustizia Ue, 22 giugno 2021, in *Rass. dir. moda e arti*, 2022, 1, p. 164). A tale riguardo, va precisato che l'attività di indicizzazione automatizzata dei contenuti caricati in piattaforma non è sufficiente ad integrare suddetta "conoscenza", al pari della generica consapevolezza che la piattaforma sia utilizzata anche per condividere contenuti che possono violare diritti di proprietà intellettuale.

43 Così, Cass., 19 marzo 2019, n. 77008, cit.

Con specifico riferimento al caso in cui il danno discenda dal trattamento dei dati, posto che il provider risulterà tendenzialmente titolare, ovvero responsabile[44], del trattamento, bisognerà distinguere: il provider passivo potrà andare esente da responsabilità, ai sensi degli artt. 14 ss d. lgs. 70/2003, mentre il gestore attivo andrà sottoposto alla applicazione delle regole comuni di cui agli art. 1218, ovvero 2043 c.c. (a seconda del regime di responsabilità in rilievo, secondo quanto già osservato nel paragrafo precedente).

Una volta accertata la responsabilità del fornitore di servizi, una peculiare attenzione andrà rivolta alla quantificazione dei danni. L'individuazione dei parametri per la liquidazione impone all'interprete una presa d'atto della oramai acclarata polifunzionalità della responsabilità civile, che, nell'ottica di garantire una tutela effettiva al danneggiato, assume una coloratura anche sanzionatoria e deterrente, oltre che compensativa[45].

A tal fine, appare essenziale considerare la peculiarità dell'illecito commesso via internet. La potenzialità lesiva che caratterizza qualsivoglia condotta in grado di incidere su diritti della personalità altrui[46], invero, nel caso che ci occupa risulta esponenzialmente acuita dalla specificità del contesto della rete: l'assenza di confini spaziali[47], da un lato, e la rapidità di propagazione dell'illecito, dall'altro, determinano l'opportunità di predisporre reazioni effettive, in grado di assicurare un ristoro pieno degli interessi lesi, e, al contempo, fungere da deterrente in un'ottica general preventiva.

Sul punto, va rammentato che, anche sotto la normativa previgente alla emanazione del GDPR, pur nel formale ripudio della logica del danno "in re

44 L'indagine circa la qualifica del provider dovrà necessariamente essere compiuta caso per caso. Ad esempio, il fornitore del servizio di "web hosting" è sicuramente "responsabile del trattamento" per conto del gestore del sito, che è "titolare del trattamento". Il "cloud provider" – stando ad un recente parere del Garante sloveno per la protezione dei dati (IP – 0612-23/2019/19) – si qualifica come contitolare del trattamento con il cliente, e non un mero responsabile. Quanto ai social networks, l'EDPB ha emanato delle linee guida (n. 8/2020), in cui si rileva che l'inserzionista e il fornitore di social media operano congiuntamente nel caso di display advertising mirato e devono, conseguentemente, qualificarsi come contitolari. Con riguardo al rapporto tra social network e gestore di una pagina amministrata da un diverso soggetto, la Corte di Giustizia (sentenza del 5 giugno 2018, C-210/16) ha stabilito che gli amministratori di "Fanpage" su Facebook debbano essere considerati "contitolari del trattamento" insieme a Facebook stesso, in relazione al trattamento posto in essere tramite l'utilizzo di tali pagine social.

45 Cfr., per gli opportuni riferimenti dottrinali, la nota n. 52.

46 In dottrina si è puntualizzato che il trattamento illecito dei dati personali ha una caratterizzazione plurioffensiva, essendo idoneo a ledere, al contempo, molteplici interessi della persona (quali il diritto alla riservatezza, alla identità personale, protezione dei dati personali, immagine e dell'oblio). Così, Tosi, E.: "Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE", *Danno resp*., 2020, 4, p. 435, e dottrina ivi citata; in arg., cfr. anche Bessone, M. e Cassano, G.: *Diritto industriale e diritto d'autore nell'era digitale*, Giuffré, Milano, 2022.

47 In arg., Irti, N.: *Norma e luoghi. Problemi di geo-diritto*, Ed. Laterza, Roma-Bari, 2006, p. 5; Id., *L'ordine giuridico del mercato*, Ed. Laterza, Roma-Bari, 2009, p. 150, rileva che "lo spazio telematico è sciolto dalla fisicità: non tanto sta oltre i confini territoriali, quanto non ha confini".

ipsa"[48], non di rado la giurisprudenza tendeva ad accordare il risarcimento per l'illecito trattamento dei dati sulla scorta di un meccanismo di tipo presuntivo, volto a riconnettere la sussistenza del pregiudizio alla peculiare connotazione della condotta, ovvero alla tipologia dell'interesse leso. Si consideri il caso[49] – ampiamente noto – in cui la violazione della privacy di un celebre calciatore veniva "compensata" con un risarcimento di importo cospicuo (due milioni in primo grado, ridotti a 70.000 euro in appello[50]), pur in assenza della prova del danno, solo in considerazione del rilievo che le condotte fossero "particolarmente riprovevoli per il loro carattere subdolo e sleale", nonché volte al distorto impiego dello strumento telefonico per il raggiungimento di finalità illecite. Ad analoghe considerazioni è giunta la stessa corte di legittimità, laddove ha ricondotto la sussistenza del danno non patrimoniale alla mera "violazione delle regole di correttezza e di liceità, le quali sono finalizzate a bilanciare la libertà di chi tratta i dati con la preservazione della sfera del danneggiato"[51].

Ne risulta, dunque, una curvatura in senso "sanzionatorio" del risarcimento, conseguente alla valorizzazione del rango costituzionale degli interessi lesi nel caso del trattamento dei dati personali, la quale giustifica di per sé la condanna risarcitoria, pure "in difetto di alcuna prova di una concreta alterazione delle consuetudini domestiche" dei danneggiati, onde "assicurare quella che si è giunti bensì a riconoscere che sia la valenza punitiva pure propria del risarcimento del danno non patrimoniale da lesione dei diritti fondamentali"[52].

Del resto, in talune pronunce aventi ad oggetto la responsabilità dei provider attivi, la giurisprudenza è apparsa incline a modulare il giudizio sul quantum sulla scorta del grado di antigiuridicità della condotta del gestore. Si consideri la fattispecie in cui – con riferimento alla violazione del diritto d'autore online – il Tribunale di Roma ha ritenuto di adeguare l'importo da liquidare sulla scorta della

48 Con specifico riferimento alla materia in esame, cfr. Cass. 20.5.2015, 10280; Cass. 5.9.2014, n. 18812, in *Foro it*., 2015, I, c. 152.

49 Trib. Milano, 3.9.2012, n. 9749, in *Danno resp*., 2013, 51.

50 App. Milano, 22.7.2015, in *Danno resp*., 2015, p. 1047, in cui si legge significativamente che "senza dubbio le condotte di cui le società per tutto quanto innanzi illustrato sono responsabili, appaiono particolarmente riprovevoli per il loro carattere subdolo e sleale e in considerazione dell'utilizzo di strumenti di cui il gestore telefonico, in posizione di particolare favore, poteva disporre in funzione dell'espletamento di un servizio pubblico e che venivano invece in maniera distorta piegati a tutt'altre finalità".

51 Cass. 4.6.2018, n. 14242, in *Giur. It, 2019*, p. 41, con riferimento ad un illecito trattamento dei dati effettuato dalla Agenzia delle Dogane, responsabile di aver comunicato dati sensibili relativi alle vicende giudiziarie di un dipendente per il tramite di un protocollo ordinario aperto a tutti. Si legge in motivazione che "la fattispecie delineata dai due commi dell'art.15 del D. Lgs. N. 196/2003 pone quindi due presunzioni: [...] e quella secondo la quale le conseguenze non patrimoniali di tale danno [...] sono da considerare in re ipsa a meno che il danneggiante non dimostri che esse non vi sono state [...]. Ed infatti il danno maggiormente connaturato all'illecito trattamento è proprio quello non patrimoniale sicché il non avere adottato le misure idonee ad evitarlo si rivela in sostanza, come una violazione delle regole di correttezza e di liceità le quali sono finalizzate a bilanciare la libertà di chi tratta i dati con la preservazione della sfera del danneggiato".

52 Trib. Catania, 31.1.2018, n. 466, relative alla lesione del diritto, costituzionalmente garantito, alla tutela del proprio domicilio.

"condotta tenuta dal contraffattore, dalla reazione più o meno repentina nella rimozione dei materiali illecitamente veicolati e quindi, a contrario, dalla gravità e durata della condotta omissiva perpetrata a danno del titolare della privativa"[53].

L'accento, nella liquidazione, sul grado di antigiuridicità della condotta del provider e sulla peculiarità dell'interesse leso (idoneo ad essere risarcito in re ipsa), in definitiva, costituisce un ulteriore punto di emersione della "polifunzionalità" del rimedio aquiliano[54], che, nella fattispecie in esame, si presta a garantire adeguata tutela ai diritti della personalità degli utenti della rete, oltre che fungere da impulso per una responsabilizzazione dei provider in ottica sistemica.

V. ILLECITO TRATTAMENTO DATI E *BLOCKCHAIN*.

Ancora più fitti sono gli interrogativi che si pongono quando il trattamento illecito avvenga nell'ambito di una Blockchain[55]. In questo caso, invero, le criticità investono la stessa compatibilità della disciplina di cui al reg. 679/2016 con l'architettura del Registro distribuito[56].

Va rilevato che, ad onta dell'intento dei suoi ideatori, la Blockchain non costituisce un sistema impermeabile all'applicazione delle regole predisposte dall'ordinamento giuridico, ma necessita di essere inquadrata – e, dunque, regolamentata – sulla scorta delle categorie tradizionali[57]. In tale quadro, il GDPR risulta astrattamente applicabile con riguardo al trattamento dei dati registrati nel ledger, posto che questi ultimi – pur essendo crittografati – non risultano

53 Così, Trib. Roma, 10.1.2019, in *Dir. internet*, 2019, p. 140.

54 Su cui, ex multis, cfr. Salvi, C.: *La responsabilità civile*, in *Tratt. dir. privato* Iudica-Zatti, Milano, 2019, p. 11; Alpa, G.: *La responsabilità civile. Parte generale*, Utet giuridica, Torino, 2010, p. 159; Trimarchi, P.: *La responsabilità civile: atti illeciti, rischio, danno*, Giuffré, Milano, 2019, p. 283; Di Majo, A.: "Principio di legalità e di proporzionalità nel risarcimento con funzione punitiva", *Corr. giur.*, 2017, p. 1042; Monateri, P. G.: "Le Sezioni Unite e le funzioni della responsabilità civile", *Danno e resp.*, 2017, p. 419; Ponzanelli, G.: "Polifunzionalità della responsabilità civile tra diritto internazionale privato e diritto privato", *ivi*, p. 435; Scognamiglio, C.: "Le Sezioni Unite ed i danni punitivi tra legge e giudizio", *Resp. civ. prev.*, 2017, 4, p. 1109B; Perlingieri, P.: "Le funzioni della responsabilità civile", *Rass. Dir. civ.*, 2011, 1, p. 115; Id.: "La responsabilità civile tra indennizzo e risarcimento", *Rass. dir. civ.*, 2004, 4, p. 1063; Id., *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, IV, *Attività e responsabilità*, Esi, Napoli, 2020, p. 406.

55 Va, ad ogni modo, rilevato che, accanto agli elementi di frizione rispetto alla tutela dei dati, si annoverano pure vantaggi derivanti dall'impiego della Blockchain, ai fini di un sicuro trattamento. Basti pensare alla garanzia di integrità (art. 5, lett. f), trasparenza (art. 5, lett. a), tracciabilità dei dati, così come alla possibilità di accesso agli stessi (art. 15). Cfr…

56 *Ex multis*, Berberich-Steiner, M: "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?", *European Data Protection Law Review*, 2016, 2, p. 422; Palladino, A.: "L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance", *MediaLaws - Riv. dir. media*, 2019, p. 150; Frezza, G.: "Blockchain, autenticazione e arte contemporanea", *Dir. fam. pers.*, 2020, p.489; Rampone, F.: "I dati personali in ambiente blockchain tra anonimato e pseudonimato", *Ciberspazio e dir.*, 2018, p. 459.

57 Sul tema, sia consentito il rinvio a Iorio, C.: "Blockchain e diritto dei contratti: criticità e prospettive", *Actualidad juridica iberoamericana*, 2021, p. 656.

tecnicamente anonimi[58], ma pseudonimi[59]. E tuttavia, al di là di tale notazione, emerge una irriducibile distonia tra l'impianto del *Distributed ledger* – improntato alla massima decentralizzazione – e la struttura centralizzata del Reg. 679/2016.

1. I principi di minimizzazione e data protection by design.

La struttura della Blockchain appare difficilmente compatibile con taluni dei capisaldi su cui si fonda l'attuazione del principio dell'accountability nel reg. 679/2016, e che risultano essenziali per garantire la sicurezza del trattamento.

Si consideri, anzitutto, il principio di "minimizzazione", di cui all'art. 5, comma 1, lett. c), il quale impone che i dati siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". Tale requisito contrasta con la natura distribuita della Blockchain, in cui i dati sono replicati in ogni server. Altrettanto potrebbe concludersi con riguardo al principio della limitazione del trattamento (art. 18).

Ma si pensi, ancora, a taluni dei fondamentali diritti dell'interessato, quale quello alla rettificazione (art. 16) e alla cancellazione dei dati (art. 17), che appaiono difficilmente esercitabili nel contesto della catena di blocchi che, come noto, si caratterizza per la immutabilità delle informazioni registrate.

Va verificata, allora, l'esistenza di espedienti tecnici in grado di garantire l'attuazione di tali disposizioni regolamentari.

Quanto ai principi di minimizzazione e limitazione del trattamento, sono state sperimentate soluzioni che – aggiungendo "rumore" ai dati, o rendendo più difficoltosa l'associazione di una chiave privata e dati inseriti[60] – possono rivelarsi utili allo scopo. Parrebbe auspicabile, a tal fine, anche l'impiego di c.d. "indirizzi usa e getta"[61], che consentono la creazione di un nuovo indirizzo e una nuova password per ciascuna transazione.

58 Il GDPR, come noto, non trova applicazione nel caso di dati anonimi, vale a dire a "informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato" (considerando 26 GDPR).

59 Vi è sempre, infatti, la possibilità, attraverso apposite tecniche, della re-identificazione. Cfr. Faini, F: "Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection, *Resp. civ. prev.*, 2020, p. 297; Gambino, A. – Bomprezzi, C.: "Blockchain e protezione dei dati personali", *Dir. inf.*, 2019, p. 619;

60 Le soluzioni proposte, nel dettaglio, comprendono l'impiego di: a) "Zero-knowledge proofs", una tecnica che consente ad un dato soggetto di acquisire la prova di una data statuizione, senza garantire accesso ai dati sottostanti; b) aggiunta di "rumore" ai dati, consistente nel raggruppare un dato numero di transazioni tra loro, cosicché sia impossibile discernere l'identità di parte delle stesse; c) "ring signature", vale a dire un tipo speciale di firma digitale che, dato un gruppo di utenti muniti di chiavi pubbliche e private, permette di associare la transazione al gruppo in modo generico, senza rilevare l'identità dell'utente firmante. Cfr, in tema, Finck, M., "Blockchains and Data Protection in the European Union", *European Data Protection Law Review*, 2018, p.15. Tali riflessioni sono riprese da Gambino, A. M. - Bomprezzi C., *op. cit.*, p. 622.

61 *Ibidem*.

Più complesso è il tentativo di conciliare la Blockchain con l'esercizio del diritto alla cancellazione e alla rettificazione dei dati. Esiste, allo stato, la possibilità tecnica di agire sui blocchi, modificandoli[62], ma tale soluzione rischia di minare la fiducia degli utenti verso il sistema della Blockchain, il cui impiego si giustifica proprio in ragione della garanzia di certezza e immodificabilità delle informazioni registrate *on chain*.

Va prestata adesione, allora, alla tesi di chi propone di interpretare la "cancellazione" dei dati nel senso, più generico, di rendere gli stessi "inaccessibili". Nel caso in cui sia richiesto l'esercizio del diritto all'oblio, l'informazione potrebbe essere resa irraggiungibile mediante la distruzione della chiave privata[63]. Ancora più convincente è la prospettazione di un database "off-chain", all'interno del quale conservare i dati personali, i quali risulterebbero collegati alla Blockchain (e, quindi, non registrati sui blocchi) tramite un hash: in tal modo, il dato personale potrebbe essere cancellato, ovvero rettificato, senza alterare la funzione algoritmica, che resterebbe immutata nel libro mastro digitale[64].

2. La identificazione del titolare e del responsabile del trattamento.

Pur esistendo, dunque, delle soluzioni tecniche in grado di assicurare il rispetto della privacy by design e by default nella Blockchain, la più evidente criticità consiste nella difficile individuazione dei soggetti in grado di garantire la sicurezza del trattamento dei dati. Stante l'assenza di una autorità centrale dotata di poteri di controllo, non appare agevole la determinazione dei soggetti cui attribuire la qualifica titolare e del responsabile del trattamento, nel contesto del Registro distribuito.

Diverse sono le soluzioni suggerite dalla dottrina e dalle Autorità nazionali di protezione dei dati personali, con riferimento alle Blokchain permissionless.

Quanto al titolare del trattamento, si tende ad escludere che tale ruolo possa essere svolto dagli sviluppatori del *software* – posto che gli stessi non hanno potere di decidere le finalità o i mezzi del trattamento – ovvero dai *miners*, i quali si limitano a partecipare al processo di validazione delle transazioni e, quindi, di formazione dei bocchi, senza influire nella determinazione delle finalità del trattamento[65].

62 Diverse sono le soluzioni tecniche in grado di rendere i dati registrati "onchain" modificabili: si va dalla funzione di "chamelon hashes", alla tecnica del "pruning" (che consente di eliminare un dato, quando lo stesso non risulta più necessario), o a quella del "fork", che conduce alla rideterminazione delle regole della catena, con la creazione di un nuovo ledger. Cfr, in tema, Finck, M., *op. cit.*, p. 15.

63 Tale soluzione è stata suggerita dal CNIL francese: "Solutions for a responsible use of the blockchain in the context of personal data", in https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

64 Questa soluzione potrebbe essere raggiunta per mezzo dell'impiego del protocollo IPFS ("InterPlanetary File System"), il quale include "on chain" solo il link ai dati, in aggiunta ad una marcatura temporale ("timestamp") e a un hash dei dati esternalizzati. Cfr. Finck, M., *op. cit.*, p. 15.

65 In arg., Bellomia, V: "Il contratto intelligente: questioni di diritto civile", in www.judicium.it

Da più parti, si sostiene che titolari sarebbero – ciascuno nei confronti degli altri – i nodi che partecipano alla transazione, posto che la scelta, da parte del singolo utente, di impiegare proprio una blockchain per effettuare una ben precisa operazione economica integra la determinazione – rispettivamente – dei mezzi e delle finalità del trattamento dei dati[66]. Dovrebbero, invece, qualificarsi come responsabili i nodi che, non partecipando alla transazione, mantengono una copia dei dati.

Meno difficoltosa parrebbe la qualifica di responsabile del trattamento, che potrebbe spettare agli sviluppatori degli smart contracts – deputati ad elaborare i dati per conto degli utenti, titolari del trattamento – ovvero ai miners, i quali, validando le transazioni contenenti dati personali, con tutta evidenza "trattano i dati per conto del titolare del trattamento"[67].

E tuttavia, pur potendosi astrattamente procedere alla attribuzione delle qualifiche rilevanti ai fini del GDPR, sta di fatto che le caratteristiche della Blockchain permissionless rendono estremamente ostico l'adempimento dei penetranti obblighi di condotta previsti dal Regolamento. Da un lato, la globalità del registro ostacola il monitoraggio della totalità delle transazioni aggiunte nei blocchi; ma, soprattutto, lo pseduonimato delle identità impedisce agli utenti di identificare il titolare, e a quest'ultimo di individuare l'utente destinatario di precisi obblighi di condotta.

Allo stato, dunque, parrebbe che la sola tecnologia integralmente compatibile con il quadro giuridico di riferimento sia quella della Blockchain permissioned. In tal caso, invero, ravvisandosi un soggetto che determina le regole di accesso al sistema, i ruoli di cui al GDPR sono facilmente identificabili: proprio l'autorità centrale deputata alla determinazione dei criteri di selezione dei nodi, degli aggiornamenti del sistema, e delle regole di trasparenza, invero, dovrebbe assumere la qualifica di "titolare del trattamento". L'adozione, poi, delle soluzioni in grado di assicurare la minimizzazione, la rettificazione e la cancellazione dei dati parrebbero garantire una tendenziale compatibilità con il GDPR.

VI. CONSIDERAZIONI CONCLUSIVE.

Il presente contributo ha inteso esaminare talune delle criticità connesse alla circolazione e al trattamento dei dati nell'era digitale. Nel complesso, se ne

66 Fink, M: "Blockchains and Data Protection in the European Union", in *European Data Protection Law Review*, 2018, p.17; in tal senso anche il CNIL francese, "Solutions for a responsible use of the blockchain in the context of personal data", cit. In senso critico, Bellomia, V: "Il contratto intelligente: questioni di diritto civile", cit., p. 12, la quale rileva che questa tesi – determinando una "responsabilità diffusa", comporterebbe per qualsiasi intervento sul trattamento (quale la rettifica di un dato) il necessario consenso della maggioranza dei nodi, in quanto tutti contitolari di ogni trattamento, con l'effetto di paralizzare il sistema.

67 Questa è l'opinione espressa dal CNIL, "Solutions for a responsible use of the blockchain in the context of personal data", cit.

ricava un quadro disciplinare tutt'altro che definito. Le incertezze circa la natura giuridica del dato personale si riflettono sulle perplessità riguardo le regole per la circolazione dello stesso e le tutele esperibili da parte dell'interessato in caso di violazione.

Nell'ottica di garantire una tutela sempre più estesa agli interessati vanno guardate con favore le innovazioni introdotte dai due recenti Regolamenti del Digital Services Act[68] e Digital Market Act[69].

Al fine di combattere l'opacità delle scelte algoritmiche anche in relazione all'impiego dei dati, il primo atto prevede obblighi specifici per le piattaforme in punto di informazione e di trasparenza. Si richiede, in particolare, che agli utenti siano rese conoscibili le regole circa il funzionamento di sistemi di moderazione e di raccomandazione dei contenuti, nonché di pubblicità online. Significativamente, si introducono divieti di utilizzo delle pratiche ingannevoli volte a manipolare le scelte degli utenti, e di pubblicità mirata rivolta ai minori o basata sui dati sensibili degli utenti. Si introduce, in capo alle piattaforme, pure l'obbligo di abilitazione degli utenti al blocco delle "raccomandazioni" basate sulla profilazione.

Il Digital Market Act completa il piano delle tutele, guardando al possibile impiego dei dati, da parte del "gatekeeper"[70], per finalità distorsive della concorrenza nel mercato. Si spiegano, così, i nuovi divieti di limitare o rifiutare la portabilità dei dati o il riuso dei dati, al fine di scoraggiare o impedire all'utente di abbandonare la piattaforma; si contempla, ancora, il divieto di combinazione di dati personali dell'utente, ricavati dai servizi di piattaforma, con altri dati personali ricavati da altri servizi, anche di terze parti, senza espressa autorizzazione dell'utente stesso. È significativo pure l'obbligo di fornire a titolo gratuito agli utenti commerciali un accesso efficace, continuo e in tempo reale a dati aggregati e non aggregati forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base (sempre previo consenso dell'utente).

Tali Regolamenti, letti unitamente alla disciplina del GDPR, costituiscono un ulteriore tassello del disegno di quella "tutela multilivello" dell'utente digitale che, come si è rilevato, appare imprescindibile ai fini di una piena attuazione dell'effettività della protezione dei diritti fondamentali nella società tecnologica.

68 Reg. (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali).

69 Reg. (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

70 I "Gatekeeper" sono le categorie soggettive di piattaforme soggette all'applicazione del Digital Market act. La designazione come gatekeeper avviene sulla base di criteri qualitativi e soggettivi, oltre che in riferimento ai tipi di servizi offerti (ovvero se eroganti i cosiddetti "Core Platform Services"), secondo le soglie di cui all'art. 3 del Regolamento.

BIBLIOGRAFIA

Alpa, G.: *La responsabilità civile. Parte generale*, Utet giuridica, Torino, 2010

Bellomia, V: "Il contratto intelligente: questioni di diritto civile", in www.judicium.it

Berberich-Steiner, M: "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?", *European Data Protection Law Review*, 2016, 2, p. 422

Bessone, M. e Cassano, G.: *Diritto industriale e diritto d'autore nell'era digitale*, Giuffré, Milano, 2022

Bianca, C. M. -Busnelli, F. D. (a cura di), *La protezione dei dati personali. Commentario al d. lgs. 30 giugno 2003, n. 196 (« Codice della privacy »)*, I, Cedam, Padova, 2009

Bocchini, F.: "La responsabilità civile plurisoggettiva, successiva ed eventuale dell'ISP", *Giur.it.*, 2019, p. 2604

Bocchini, F.: "Responsabilità dell'hosting provider, la responsabilità di Facebook per la mancata rimozione di contenuti illeciti", *Giur. it.*, 2017, p. 629

Bravo, F.: "Lo «scambio di dati personali» nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto", *Contr. e impr.*, 2019, p. 34;

Bravo, F.: "Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali", in *Persona e mercato dei dati. Riflessioni sul GDPR* (a cura di N. Zorzi Galgano), Wolters Kluver, Milano, 2019, p. 393

Busnelli, F. D.: "Itinerari europei nella «terra di nessuno tra contratto e fatto illecito»: la responsabilità da informazioni inesatte", *Contr. impr.*, 1991, p. 539

Calzolaio, S.: "Introduzione. Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati", *Riv. it. inf. e dir.*, 2021, p. 7

Calzolaio, S.: "Protezione dei dati personali" (voce), *Dig. disc. pubbl.*, 2017, p. 594

Camardi, C.: "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", *Giust. civ.*, 2019, p. 499

Caringella, F.: "La tutela aquiliana della privacy nel codice per la protezione dei dati personali (d. lgs. n. 196/2003), in Id., *Studi di diritto civile*. III. *Obbligazioni e responsabilità*, Giuffré, Milano, 2005, p. 715

Cassano, G.: "La Cassazione civile si pronuncia sulla responsabilità dell'internet service provider", *Dir. ind*., 2019, 4, p. 35

Castronovo, C: "Situazioni soggettive e tutela nella legge sul trattamento dei dati personali", *Eur. dir. priv*., 1998, p. 656

Castronovo, C.: *Responsabilità civile*, Giuffré, Milano, 2018

Cuffaro, V. -D'Orazio, G. -Ricciuto, V. (a cura di): *Il Codice del trattamento dei dati personali*, Giappichelli, Torino, 2007

Cuffaro, V.: "A proposito del ruolo del consenso", in *Trattamento dei dati e tutela della persona* (a cura di V. Cuffaro, V. Ricciuto, V. Zeno Zencovich,) Giuffré, Milano, 1999, p. 121

Cuffaro, V.: "Il diritto europeo sul trattamento dei dati personali", *Contr. impr*., 2018, 3, p. 1098;

D'Acquisto, G.: "Intelligenza artificiale", in *I diritti nella "rete" della rete. Il caso del diritto d'autore"* (dir. da F. Pizzetti), Giappichelli, Torino, 2021, p. 127

De Franceschi, A.: *La circolazione dei dati personali tra privacy e contratto*, Napoli, Esi, 2017

Di Ciommo, F.: "Oltre la direttiva 2000/31/Cee, o forse no. La responsabilità dei provider di Internet nell'incerta giurisprudenza europea", *Foro it*., 2019, I, p. 2078

Di Majo, A.: "Principio di legalità e di proporzionalità nel risarcimento con funzione punitiva", *Corr. giur*., 2017, p. 1042

Faini, F: "Blockchain e diritto: la «catena del valore» tra documenti informatici, smart contracts e data protection, *Resp. civ. prev*., 2020, p. 297

Finck, M., "Blockchains and Data Protection in the European Union", *European Data Protection Law Review*, 2018, p.15

Finocchiaro, G.: "Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali", in *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 ago- sto 2018, n. 101*, (a cura di G. Finocchiaro), Zanichelli, Bologna, 2019, p. 5

Frezza, G.: "Blockchain, autenticazione e arte contemporanea", *Dir. fam. pers.*, 2020, p.489

Gambini, M. L.: "La responsabilità dell'internet service provider approda in Cassazione", *Corr. giur.,* 2020, 2, p. 177

Gambino, A. – Bomprezzi, C.: "Blockchain e protezione dei dati personali", *Dir. inf.*, 2019, p. 619

Giampiccolo, G.: "La tutela giuridica della persona umana e il c.d. diritto alla riservatezza", *Riv. trim. dir. e proc. civ.*, 1958, p. 458

Iorio, C.: "Blockchain e diritto dei contratti: criticità e prospettive", *Actualidad juridica iberoamericana*, 2021, p. 656

Irti, N.: *Norma e luoghi. Problemi di geo-diritto*, Ed. Laterza, Roma-Bari, 2006

Irti, N.: *L'ordine giuridico del mercato*, Ed. Laterza, Roma-Bari, 2009

Messinetti, R.: "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali", *Riv. crit. dir. priv.*, 1998, p. 35

Monateri, P. G.: "Le Sezioni Unite e le funzioni della responsabilità civile", *Danno e resp.*, 2017, p. 419

Oppo, G.: "«Trattamento» dei dati personali e consenso dell'interessato", in Id., *Scritti giuridici*, VI, *Principi e problemi del diritto privato*, CEDAM, Padova, 2000, p. 113

Palladino, A.: "L'equilibrio perduto della blockchain tra platform revolution e GDPR compliance", *MediaLaws - Riv. dir. media*, 2019, p. 150

Patti, S.: "Il consenso dell'interessato al trattamento dei dati personali", *Riv. dir. civ.*, 1999, p. 455

Pellecchia, E.: "La responsabilità civile per trattamento dei dati personali", *Resp. civ. prev.*, 2006, p. 221

Perlingieri, C.: *Profili civilistici dei social networks,* Napoli, Esi, 2014

Perlingieri, P: "L'incidenza dell'interesse pubblico sulla negoziazione privata", *Rass. dir. civ.*, 1986, 4, p. 57

Perlingieri, P.: "La responsabilità civile tra indennizzo e risarcimento", *Rass. dir. civ.*, 2004, 4, p. 1063;

Perlingieri, P.: "Le funzioni della responsabilità civile", *Rass. Dir. civ.*, 2011, 1, p. 115;

Perlingieri, P.: *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, IV, *Attività e responsabilità*, Esi, Napoli, 2020, p. 406

Piraino, F.: "Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato", *Nuove leggi civ. comm.*, 2017, p. 369;

Ponzanelli, G.: "Polifunzionalità della responsabilità civile tra diritto internazionale privato e diritto privato", *Danno e resp*, p. 435

Pugliese, G.: "Il diritto alla riservatezza nel quadro dei diritti della personalità", *Riv. dir. civ.*, 1963, p. 605.

Rampone, F.: "I dati personali in ambiente blockchain tra anonimato e pseudonimato", *Ciberspazio e dir.*, 2018, p. 459

Renna, M.: "Sicurezza e gestione del rischio nel trattamento dei dati personali", *Resp. civ. prev.*, 2020, p. 1343

Rescigno, P.: "*Il diritto all'intimità della vita privata*", in *Studi in onore di F. Santoro-Passarelli*, IV, Jovene, Napoli, 1972, p. 121

Ricciuto, V.: "Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali", *Riv. dir. civ.*, 2020, 3, p. 642

Rodotà, S.: "Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali", *Riv. crit. dir. priv.*, 1997, p. 583

Roppo, V.: "La responsabilità civile per trattamento di dati personali", *Danno resp.*, 1997, p. 663

Salvi, C.: *La responsabilità civile*, in *Tratt. dir. privato* Iudica-Zatti, Milano, 2019

Sciascia, G.: "Reputazione e potere: il social scoring tra distopia e realtà", *Giorn. dir. amm.*, 2021, 3, p. 317

Scognamiglio, C: "Buona fede e responsabilità civile", *Eur. dir. priv.*, 2001, p. 357

Scognamiglio, C.: "Le Sezioni Unite ed i danni punitivi tra legge e giudizio", *Resp. civ. prev.*, 2017, 4, p. 1109B

Sica, S. – Stanzione, P. (a cura di): *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Zanichelli, Bologna, 2005

Solinas, C.: "Circolazione dei dati personali, onerosità del contratto e pratiche commerciali scorrette", *Giur. it.*, 2021, p. 325

Soro, A.: "La protezione dei dati personali nell'era digitale", *Nuova giur. civ. comm.*, 2019, 2, p. 343

Tosi, E.: "Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE", *Danno resp.*, 2020, 4, p. 435

Trimarchi, P.: *La responsabilità civile: atti illeciti, rischio, danno*, Giuffré, Milano, 2019

Visintini, G: "Dal diritto alla riservatezza alla protezione dei dati personali", *Dir. inf.* e *informatica*, 2019, p. 1.

Zecchin, F: "Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali", *Eur.* e *dir. priv.*, 2022, p. 517.

Zeno-Zencovich, V.: "Do "Data Markets" Exist?", *MediaLaws*, 2019, p. 26