ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

18 DICEMBRE 2019

La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato

di Dimitri De Rada
Avvocato presso il Foro di Milano

La responsabilità civile in caso di mancato rispetto del GDPR. Privacy by default, privacy by design e accountability nell'ottica del Diritto Privato *

di Dimitri De Rada
Avvocato presso il Foro di Milano

Il 25 maggio 2018 è divenuto applicabile il c.d. GDPR, General Data Protection Regulation, Regolamento UE 679/2016, ossia il Regolamento con cui la UE disciplina la materia del trattamento dei dati personali abrogando la Direttiva 95/46/CE.

La digitalizzazione della società e dell'economia sta producendo un impatto diversificato (anche) sull'impegno civico nel processo decisionale e sulle barriere alla partecipazione pubblica ai processi democratici. L'analisi dei Big Data e i sistemi di intelligenza artificiale hanno reso possibile la raccolta, la combinazione, l'analisi e l'archiviazione illimitata di volumi enormi di dati. Negli ultimi vent'anni è emerso un modello economico dominante per la maggior parte dei servizi basati sul web, fondato sul tracciamento online delle persone e sulla raccolta di dati sul carattere, la salute, le relazioni nonché i pensieri e le opinioni, con il fine di generare introiti mediante la pubblicità digitale. Tali mercati digitali si sono concentrati nelle mani di un numero esiguo di società, che esercitano una vera e propria funzione di controllo in Internet e hanno valori di capitalizzazione di mercato, adeguati all'inflazione, superiori a quelli di qualsiasi altra società che la storia ricordi. Questo ecosistema digitale, in cui oltre il 50 % della popolazione è presente su Internet, ha collegato persone di tutto il mondo, sebbene in modo molto difforme in termini di geografia, ricchezza e genere1: Basterebbero queste considerazioni (svolte dal GARANTE EUROPEO DELLA PROTEZIONE DEI DATI) a far comprendere l'importanza del GDPR e la sua necessità.

Sebbene sia un atto di natura europea, il Regolamento ha già influenzato le *policies* in materia di trattamento dati di aziende multinazionali il cui mercato non è circoscritto alla sola Unione Europea e con sede al di fuori di tale territorio, infatti la portata operativa del Regolamento è tale da poter essere indicato -nei fatti

* Articolo sottoposto a referaggio.

[1]Cit. GARANTE EUROPEO DELLA PROTEZIONE DEI DATI *"Sintesi del parere del GEPD su manipolazione online e dati personali"* (Il testo integrale del presente parere è disponibile in inglese, francese e tedesco sul sito web del GEPD www.edps.europa.eu) (2018/C 233/06) Su G.U. Dell'Unione Europea 4 luglio 2018

- come l'International Legal Standard per il trattamento dei dati personali. 2 *"Mass adoption of GDPR privacy standards by international companies have been cited as an example of the "Brussels effect", a phenomenon wherein European laws and regulations are used as a global baseline due to their gravitas*"[3] Lo scopo della normativa è allo stesso tempo armonizzare le regole tra gli Stati membri dell'UE, facilitare il libero flusso di dati personali -facilitando così gli scambi in un Digital Single Market (DSM) - e garantire i diritti fondamentali dei titolari dei dati.

Innanzitutto, il GDPR stesso prevede che esso venga applicato anche *"al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*

- *l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*
- *b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione"* (art. 3)[4].

[2] *"The European Union's new data protection law is the reason behind recent privacy updates from several tech platforms. Major multinational companies are reviewing their privacy terms to adhere to the General Data Protection Regulation (GDPR) that goes into effect later this month. Although the rights granted by the law do not extend to people living outside the EU, some companies prefer using a single global standard because of the logistical challenges of maintaining multiple standards. However, the broad territorial scope of the law may require all US non-governmental entities to review their web presence to determine if they are subject to GDPR",* https://regulatorystudies.columbian.gwu.edu/gdpr-does-it-matter-side-atlantic *Aryamala Prasad* GDPR: Does it matter on this side of the Atlantic?, George Washington University Regulatory Studies Center
"*For instance, unlike a directive, a regulation does not have to be implemented in the national laws of the EU Member States. Hence, the GDPR should lead to a more harmonized regime in Europe. Furthermore, the enforcement mechanisms are strengthened. Data Protection Authorities can impose fines for non-compliance of up to 4% of the worldwide turnover of companies. This also applies to, for instance, American companies operating in Europe or gathering data about people in Europe. Hence, the GDPR, the world's strictest and most comprehensive data privacy law, will influence policy worldwide.*" Sloot, Bart and Zuiderveen Borgesius, Frederik, The EU General Data Protection Regulation: A New Global Standard for Information Privacy (April 15, 2018). Available at SSRN: https://ssrn.com/abstract=3162987 or http://dx.doi.org/10.2139/ssrn.3162987

[3] Roberts, Jeff John (25 May 2018). "The GDPR Is in Effect: Should U.S. Companies Be Afraid?". Retrieved 28 May 2018. http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/;
Beata A. Safari "*Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*" 47 Seton Hall L. Rev. 809 (2016-2017)

[4] A tale proposito, si sono già avute conseguenze pratiche. Basti pensare al blocco di siti di diverse testate giornalistiche U.S.A., come Los Angeles Times e Chicago Tribune, nella data in cui il GDPR diviene applicabile, direzionando i lettori a una pagina web recante il messaggio: *"Unfortunately, our website is currently unavailable in most European countries. We are engaged on the issue and committed to looking at options that suppor our full range of digital offerings to the EU market. We continue to identify technical compliance solutions that will provide all readers with our award-winning journalism"* (A. Hern, M. Belam, *LA Times among US-based news sites blocking EU users due to GDPR*, The Guardian, 25 maggio 2018, https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times). Inoltre, sono già state intraprese azioni legali contro Google, Facebook Instagram e Whatsapp (si ricorda che le ultime due sono state acquisite da Facebook inc.) per "*consenso forzato*", ottenuto cioè attraverso pratiche che impediscono la formazione del consenso senza ingerenze esterne (Alb.Ma., , *Gdpr al via: denunciate Google e Facebook per "consenso forzato"*, Il Sole 24 ore, 25 maggio 2018, http://www.ilsole24ore.com/art/tecnologie/2018-05-25/gdpr-via-gia-denunciate-google-e-facebook-consenso-forzato-155204.shtml?uuid=AEdzcpuE).

Inoltre, la attuale connotazione spiccatamente transnazionale del mercato rende in ogni caso necessario conformarsi al GDPR anche per aziende con sede al di fuori della UE ma che operano anche all'interno di questa. Dovendo trattare anche – sebbene non esclusivamente – dati di soggetti interessati che si trovano nella UE, è necessario che questi uniformino le proprie *policies* e strutture organizzative alle disposizioni fissate dal GDPR, utilizzandole anche per il trattamento di soggetti al di fuori dell'Unione (operazione resa possibile grazie al fatto che il GDPR si qualifica ora come standard più alto in materia). Pertanto, si assiste alla diffusione di trattamenti conformi al GDPR anche in fattispecie non previste dal Regolamento stesso, segno dello sviluppo di un circolo virtuoso in cui la *best pratice* di origine UE diviene paradigma per il trattamento dei dati personali a livello mondiale.

Va sottolineato come poi l'ambito di applicazione della normativa UE è assai più ampio di quello semplicemente commerciale infatti: "Il diritto dell'UE sulla protezione dei dati e sulla riservatezza delle comunicazioni elettroniche si applica alla raccolta di dati, alla profilazione e al microtargeting e, se correttamente messo in atto, dovrebbe contribuire a ridurre al minimo i danni derivanti da tentativi di manipolazione di singoli e gruppi. I partiti politici che trattano i dati dei votanti nell'UE rientrano nell'ambito di applicazione del RGPD. "[5]

Merita di essere notato come, sebbene il GDPR abbia per oggetto il solo trattamento dei dati di persone fisiche, esista già una autorevole corrente che spinge per l'ampliamento della disciplina del GDPR ai dati delle persone giuridiche. Tale corrente dottrinale [6] (che l'Autore si sente di sposare) si basa sulla constatazione che i diritti della personalità hanno già trovato estensione agli enti collettivi. A tale proposito, si considerino la L. 31 dicembre 1996, n. 675, intitolata "tutela della persona e degli altri soggetti rispetto al trattamento dei dati personali", che già includeva tra i "soggetti interessati" le persone giuridiche o ogni altro ente o associazione (art. 1), nonché il successivo Codice per la protezione dei dati personali (d. lgs. 196/2003), il quale a sua volta specifica come il "dato personale" possa riferirsi non solo a persona fisica, ma anche a persona giuridica[7]. Fatta tale premessa, non si comprende il motivo alla base di una limitazione della tutela dei dati personali all'interno delle operazioni di trattamento dei dati alle sole persone fisiche, posto che i diritti della personalità sono ormai ricondotti dalla quasi totalità degli

[5] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI *"Sintesi del parere del GEPD su manipolazione online e dati personali"* (Il testo integrale del presente parere è disponibile in inglese, francese e tedesco sul sito web del GEPD www.edps.europa.eu) (2018/C 233/06) su G.U. Dell'Unione Europea 4 luglio 2018

[6] V. G.Alpa, *Protezione da estendere alle persone giuridiche*, Sole 24 ore, 3 maggio 2018.

[7] Sul punto, si consideri il provvedimento del Garante n. 262 del 20 settembre 2012, il quale, a fronte di quanto previsto dall'art. 40 D.L. n. 201/2011, che aveva soppresso il riferimento alle "persone giuridiche" all'art. 4 D. Lgs. n. 196/2003, sostiene come il capo 1 del Titolo X del Codice, e più correttamente le disposizioni ivi contenute che riguardassero i "contraenti", continuasse a trovare applicazione anche alle persone giuridiche, enti ed associazioni.

ordinamenti anche a persone giuridiche. Queste ultime rappresentano infatti una mera struttura, professionale e sociale, le cui attività ed operazioni sono poste in essere da persone fisiche.

Si consideri sul tema come sussista già una "zona grigia" di dati riconducibili a persone tanto fisiche quanto giuridiche e che costituiscono fonte di dubbi.

Se nel caso in cui nominativo di una persona fisica sia incluso nel nome della persona giuridica (in quanto proprietario ad esempio), l'applicazione del GDPR risulta esclusa dal già visto Considerando 14, un'ipotesi più dubbia sarebbe quella di un'e-mail aziendale, dunque strutturalmente riconducibile alla persona giuridica, solitamente usata da un dipendente (persona fisica) dell'impresa. In tale ipotesi il dato si potrebbe ritenere riconducibile alla persona fisica, quindi suscettibile di tutela tramite il GDPR.

In generale, sussistono casi in cui i trattamenti automatizzati di dati personali non operano una classificazione tra dati inerenti a persone fisiche ed a persone giuridiche, talvolta determinando l'aggiunta ai profili delle prima di informazioni attinenti alle seconde. In tali ipotesi, sembrerebbe opportuno considerare i dati nel loro complesso in quanto personali e propri delle persone fisiche.

Ulteriore dettaglio significativo del GDPR è l'attenzione posta al trattamento automatizzato dei dati personali, ossia quel trattamento in grado di concludersi con decisioni proprie di una macchina anziché dell'uomo. Infatti, l'art. 22 ribadisce come "*l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (…) che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*" (art. 22 GDPR), dove come "trattamento automatizzato" vengono intese (principalmente) le "Intelligenze Artificiali" il che impegna anche i progettisti ad una "Transparent, Explainable, and Accountable AI"[8].

La disciplina del GDPR si inserisce in un contesto socio-economico in cui i dati e il loro trattamento sono caratterizzati da una natura particolare e quasi duplice. La tutela dei dati personali è un diritto riconosciuto (basti pensare all'art. 1 GDPR, che "*protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali*"); al contempo, però, oggi si ammette la natura dei dati personali come oggetto di contratto, anche con scopo di lucro – è per tale ragione che si prevede la possibilità di libera circolazione dei dati personali nell'Unione che "*non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*" (art. 1 GDPR). Non vi è

[8] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). "*Transparent, explainable, and accountable AI for robotics*". Science Robotics, 2(6), eaan6080. https://philarchive.org/archive/WACTEA

dubbio che il diritto alla riservatezza e alla protezione dei dati siano diritti fondamentali9 e che acceda quindi alla tutela "multilivello" propria di tali diritti.[10]

Si vuole ricordare come la Corte di Giustizie UE abbia qualificato il diritto alla protezione dei dati come diritto fondamentale prima ancora che il riconoscimento avvenisse a livello normativo.[11]

Il GDPR recepisce questa duplice natura del dato – diritto fondamentale e oggetto del contratto come fattore produttivo[12] – e ne disciplina conformemente il trattamento. Si nota, infatti, come, da un lato, il GDPR assicuri libertà agli interessati del trattamento, dall'altro garantisca la libertà ai titolari di negoziare

[9]GARANTE EUROPEO DELLA PROTEZIONE DEI DATI *"Sintesi del parere del GEPD su manipolazione online e dati personali"* (Il testo integrale del presente parere è disponibile in inglese, francese e tedesco sul sito web del GEPD www.edps.europa.eu) (2018/C 233/06) Su G.U. Dell'Unione Europea 4 luglio 2018

[10] "*L'iniziale mancanza di un catalogo europeo di diritti fondamentali spinge il giudice europeo a utilizzare due risorse: le tradizioni costituzionali comuni degli Stati membri e il catalogo della CEDU . Il processo d'integrazione europeo assume quindi una direzione circolare che collega il sistema costituzionale nazionale con la Convenzione EDU passando attraverso i trattati istitutivi così come interpretati dalla Corte di giustizia dell'Unione. Scopi, obiettivi e strumenti dei due sistemi sovranazionali sono molto diversi, ma creano una rete di protezione attraverso la loro complementarietà. Autorevole dottrina ha proprio per questo definito il sistema CEDU e quello UE come due sorelle per i meccanismi di tutela sui diritti fondamentali. Nell'evoluzione della storia dell'integrazione europea la perdita di competenza da parte degli Stati ha significato l'accrescimento di competenze dell'UE che ha iniziato così, sempre più, ad entrare nella sfera di competenza della CEDU. Pertanto, i due sistemi, in questo vortice convergente, hanno avviato il dialogo. I giudici della Corte di giustizia hanno utilizzato le disposizioni della Convenzione non tanto per un'applicazione diretta quanto come materiale di costruzione del proprio costituzionalismo dei diritti. La chiusura del cerchio tra i due sistemi è arrivata con la disposizione dell'art. 6 TUE. I tre cataloghi – costituzionale, europeo e convenzione – costituiscono oggi con tre sistemi giurisdizionali di corti (Corti costituzionali nazionali, Corte di giustizia dell'UE e Corte EDU) un sistema integrato che viene appunto definito multilivello nel quale l'attore principale è il giudice. Tale sistema è uno straordinario esperimento in continua evoluzione nel quale i diritti fondamentali hanno ormai certamente occupato uno spazio centrale costituendo un collegamento tra il livello nazionale e quello internazionale.*

[11] B.J.KOOPS, The trouble with European Data Protection Law, in International Data Privacy Law, Vol. 4, 2014, p. 250 ss.

[12] *"Oggi il concetto di dato personale si è spinto oltre le previsioni originarie, divenendo a tutti gli effetti un bene di scambio. I dati personali sono da considerare la merce del presente e del futuro al punto tale che la Commissione europea, in una recente iniziativa normativa sul cosiddetto digital content, ha proposto di estendere le garanzie dei consumatori anche agli utenti e agli abbonati di un servizio a cui, anziché il pagamento di una somma in denaro, venga richiesta la cessione dei propri dati, consacrando così il principio che si tratti a tutti gli effetti di una moneta. Questa ipotesi è stata duramente criticata qui al garante europeo della protezione dei dati. Allo stesso tempo, la visione dei dati personali come semplice merce e oggetto di scambio è ormai limitata ed è oggi evidente come essi abbiano finito per acquisire a tutti gli effetti il connotato di potere. I dati personali continuano a essere giuridicamente quelle informazioni che si riferiscono a individui identificati o identificabili; una nozione che può anche resistere sul piano normativo, ma di fatto è destinata a scomparire. Ciò accade a causa della natura di alcune informazioni (o pezzi di informazioni) aggregate e apparentemente anonime che, seppur private di alcuni elementi identificativi degli individui, sono a disposizione di soggetti pubblici e privati e possono essere comunque ritenute di carattere personale. Mentre la disciplina del passato si preoccupava di sanare perlopiù lo svantaggio nei rapporti tra Pubblica amministrazione e cittadini, focalizzandosi soprattutto sulla protezione dei diritti della personalità (immagine, identità personale, privacy, oblio), il Gdpr, pur mantenendo questi connotati, si pone su una scala più ampia, ponendo l'individuo al centro della policy e non permettendo integralmente la negoziabilità di questi diritti. Ciò avviene poiché le situazioni di possibile criticità sul piano dell'equilibrio riguardano i grandi gestori dell'informazione e la rapida evoluzione tecnologica nel campo dell'informazione dell'ultimo ventennio. In tal senso è indicativo il fenomeno dei big data, ovvero la concentrazione di informazioni nelle mani di pochi soggetti in grado di disporre di algoritmi software e apparecchiature hardware in grado di gestire e trattare una quantità di informazioni illimitate per scopi di diversa natura. G. Buttarelli, "I big data, la sicurezza e la privacy. La sfida europea del Gdpr", Formiche, 12, 2017, http://formiche.net/2017/12/big-data-la-sicurezza-la-privacy-la-sfida-europea-del-gdpr/*

la cessione dei dati, non solo per ottenere vantaggi utili alla acquisizione di beni e servizi necessari alla vita quotidiana, ma anche per scopi di lucro.[13]

Tutti gli elementi ora citati rendono tanto più significativa la materia della responsabilità per trattamento dati.

Il GDPR non disciplina esclusivamente il trattamento dei dati, ma anche le ipotesi di responsabilità per danni verificatisi nel trattamento stesso (incluse perdita, divulgazione, manipolazione arbitraria ecc.).

A tale proposito, l'art. 82 GDPR afferma il diritto in capo all'interessato dal trattamento dati ad ottenere un risarcimento in caso di danno provocato dal trattamento stesso; a tale diritto di risarcimento corrisponde, quindi, la responsabilità civile in capo a titolare e responsabile (limitata, quindi, a questi due soggetti determinati, differentemente da quanto avveniva con il Codice della Privacy, che parlava di responsabilità in capo a "chiunque" trattasse i dati personali).

La materia della responsabilità per danno da trattamento dati si interseca con la materia di progettazione dell'intero trattamento. Vengono quindi in rilievo i principi di *privacy by design*, *privacy by default* e *accountability*, così definibili:

1. Privacy by default indica come il titolare sia tenuto a tutelare gli interessati "di default", appunto, avendo tale tutela come principio fondante l'attività di impresa, "per impostazione predefinita" (art. 25). Da sottolineare come non mancherà un ruolo di "coregolamentazione" dei i codici di condotta e deontologici adottati dalle imprese o dalle associazioni (cfr. art. 40 GDPR e degli standards tecnici che verranno adottati nel corso del tempo14 infatti; *"The recently adopted General Data Protection Regulation (GDPR), a technology-neutral law, endorses self-regulatory instruments, such as certification and technical standards. Even before the adoption of the General Data Protection Regulation, standardisation activity in the field of privacy management and data security had emerged. In 2015, the European Commission issued the first standardisation request to the European Standardisation Organisations to develop privacy management standards based on art. 8 of the EU Charter of Fundamental Rights. There is a rising shift from command-and-control regulation to the inclusion of co-regulation tools in the EU data protection legislation."*[15]
2. Privacy by design indica, invece, la necessità di considerare la protezione dei dati sin dalla progettazione del trattamento, anziché introdurre tale tutela solo in un momento successivo.

[13] V. G.Alpa, *Protezione da estendere alle persone giuridiche*, Sole 24 ore, 3 maggio 2018.

[14] *Cfr. Considerando 100: "Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi".*

[15] Kamara, I., "*Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'*", in European Journal of Law and Technology, Vol 8, No 1, 2017

La definizione di tali procedure e misure, infatti, dovrebbe essere contestuale al momento in cui scopo e modalità del trattamento stesso vengono definiti, influenzando il design di tecnologie, infrastrutture e *business practice*[16]. Tale principio è uno degli aspetti più innovativi del GDPR: *"this approach transforms consumer privacy issues from a pure policy or compliance issue into a business imperative"*[17].

Il GDPR stesso, del resto, indica la necessità di predisporre misure atte alla tutela dei dati personali "fin dalla progettazione" del trattamento (art. 25 GDPR), misure che il titolare deve essere quindi in grado di provare per evitare l'obbligo di risarcimento dell'interessato danneggiato.

- *Accountability* indica "la responsabilità sociale nel dover rendere conto a terzi delle scelte che sono state compiute". Questo termine inglese rimanda quindi ai concetti di affidabilità, capacità e competenza aziendale in materia di gestione dei dati. La *accountability,* quindi, è legata strettamente alla necessità per titolare e responsabile di dimostrare la conformità al GDPR del trattamento da loro predisposto anche ai fini di dimostrare ex post la liceità della propria condotta (in conformità con l'onere probatorio proprio già previsto all'art. 2050 c.c.).

Il rischio di insorgenza della responsabilità può quindi essere limitato attraverso la progettazione di *policy* e codici di trattamento dati che minimizzino i possibili effetti di trattamenti illegittimi, con valutazioni di probabilità del rischio e gravità degli effetti in concreto. Creando il trattamento dati una presunzione di responsabilità extracontrattuale, titolari e responsabili del trattamento sono chiamati a soddisfare un molto pesante onere probatorio, essendo chiamati – come già osservato – a provare di aver adottato misure organizzative e di sicurezza efficaci e adeguate a prevenire il danno.

Pertanto, il titolare del trattamento dati deve porre in essere misure e politiche aziendali in grado di dimostrare il rispetto del GDPR (*accountability*), sin dalla progettazione dell'attività aziendale stessa (*privacy by design*), dato che la tutela dei dati personali è considerato uno dei principi sui quali si fonda l'attività di impresa del titolare (*privacy by default*).

La predisposizione del trattamento dati influenza anche l'individuazione, come possibili responsabili, dei soli titolare e responsabile del trattamento, unitamente al carattere solidale di tale responsabilità.

Viene definito titolare del trattamento "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"; per responsabile del trattamento si intende invece "la persona fisica o giuridica, l'autorità

[16]Gutwirth, S., Leenes, R., De He rt, P. (a cura di), *Reforming European data protection law* (Vol. 20), 2014, Springer.
[17]A. Cavoukian, *Privacy by Design in Law, Policy and Practice, A White Paper for Regulators, Decision-makers and Policy-makers*, Agosto 2011, Information and Privacy Commissioner, Ontario, Canada, disponibile presso: http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf

pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4 GDPR).

Quindi, i due soggetti hanno in capo differenti obblighi e in base al principio di *accountability* devono essere in grado di provarne il rispetto e da ciò deriva la ripartizione delle responsabilità prevista dall'art. 82 del Regolamento disciplina in coerenza con quanto disposto dal Considerando 79: *"La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento".*

Mentre il secondo paragrafo dell'articolo 82 del Regolamento dispone che *"Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento".*

Quindi, il titolare risponde per il danno causato da trattamento in violazione dello stesso GDPR (cioè illegittimo), mentre il responsabile risponde per il danno causato dal mancato o non corretto adempimento delle direttive e degli obblighi fissati dal titolare.

Le disposizioni di cui all'art 82 dovranno essere interpretate alla luce:

(a) per quanto riguarda il titolare, del Considerando 146: *"Ciò (la violazione del regolamento, ndr) non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento"*;

(b) per quanto riguarda il Responsabile, dell'art. 28, paragrafo 3: *"Con riguardo alla lettera h) del primo comma1, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati."*

Fattivamente, il Titolare è il soggetto che determina le modalità e la *ratio* della raccolta dei dati, seleziona quali di essi dovranno raccogliersi ed elaborarsi e statuisce chi potrà accedervi.

In base al principio di responsabilizzazione del Titolare, egli dovrà adempiere agli obblighi sanciti dalla legislazione europea, rendendosi garante dell'adeguatezza alla stessa delle misure organizzative e tecniche implementate. Più nel dettaglio, tali obblighi comprendono la consegna all'interessato di un'informativa conforme al dettato dell'art. 13, GDPR, e la definizione di una struttura societaria che consenta agli

interessati il libero esercizio dei propri diritti così come previsti dagli artt. 15 – 22, GDPR. Da evidenziarsi come il regime di responsabilità previsto dal GDPR in capo al Titolare non sia dissimile da quello della Dir. 95/46, posto che esso dipende dalla natura dell'obbligazione in questione. Peraltro, la maggioranza delle obbligazioni incluse nel GDPR sono da qualificarsi in quanto obbligazioni di mezzo (es.: art. 17 c. 2 e 25 c. 1), mentre rari sono i casi di obbligazioni di risultato (es.: art. 13 c. 3). Per quanto attiene al Responsabile, se da un lato il GDPR ha meglio precisato gli obblighi ascrivibili a tale soggetto rispetto alla previgente disciplina, dall'altro permane la medesima subordinazione alla natura dell'obbligazione, di mezzi o di risultato. A titolo di esempio, tra le prime può citarsi l'art. 32, mentre tra le seconde l'art. 29. In aggiunta, il numero delle prime si conferma decisamente superiore alle seconde[18].

Primo atto che permette la ripartizione di responsabilità tra questi due soggetti è l'atto di nomina (che può avere natura non solo di contratto, ma anche di altro atto giuridico) del responsabile da parte del titolare. La scelta del responsabile, da parte del titolare, deve essere basata sulla verifica della presenza di garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare il regolamento (art. 28 GDPR). È inoltre opportuno evidenziare come il responsabile del trattamento risponda dell'eventuale danno anche qualora non abbia agito conformemente alle istruzioni ricevute dal titolare. Sempre secondo l'art. 82 GDPR è quindi necessario che il responsabile valuti attentamente il contenuto dell'atto di nomina, che comunque deve essere conferita da parte del titolare dopo una sua attenta valutazione delle competenze e caratteristiche dei possibili responsabili del trattamento al fine di compiere una valida selezione. L'atto di nomina permette quindi di definire i limiti dell'ambito di responsabilità dei due soggetti. L'elaborazione dell'atto di nomina, che avviene al momento di progettazione delle procedure di trattamento dati, si configura quindi come un esempio della già menzionata *privacy by design*.

Il titolare, pertanto, è chiamato a una ponderata scelta del responsabile (qualora quest'ultimo venga nominato – scelta che rimane, quindi, eventuale), includendo nella propria scelta una valutazione approfondita delle caratteristiche e delle competenze del potenziale responsabile. Quest'ultimo, al contrario, dovrà esaminare attentamente l'atto di nomina col quale viene delegato dal titolare al trattamento dei dati personali.

Del resto, "la gestione a fini economici delle informazioni – ottenute nelle diverse fasi dei processi produttivi dell'impresa, o da fonti esterne – deve fondarsi su un processo di validazione che riguardi, non

[18] Per approfondimenti, si segnala Brendan Van Alsenoy, Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation, 7 (2017) JIPITEC 271 para 1.

solo la qualità e la veridicità del dato analizzato, ma anche – e, per certi versi, soprattutto – l'espletamento di una funzione di verifica e controllo dell'aderenza alle prescrizioni applicabili"[19].

Da ultimo, è opportuno soffermarsi sul peculiare onere della prova previsto in caso di azioni di responsabilità civile per danno causato dal trattamento. Infatti, l'interessato che lamenti di aver subito un danno dovrà solo provarne l'esistenza ed il rapporto causale con il trattamento illecito, mentre titolare e responsabile saranno invece chiamati a provare di aver adottato tutte le misure per evitare il danno in oggetto. Vi è quindi come già visto un'inversione dell'onere della prova, che sarà tra breve approfondito, a carico dei danneggianti, conformemente – per ciò che riguarda il diritto interno – a quanto già affermato nel Codice della Privacy.

La disciplina prevista da questo articolo è quindi accostabile a quella dell'art. 2050 Cod. Civ., rubricato "responsabilità per l'esercizio di attività pericolose"[20].

L'attività di trattamento dei dati, del resto, è sempre stata in passato qualificata come "attività pericolosa", e quindi rientrante nell'ambito di applicazione dell'art. 2050 Cod. Civ: infatti L'art. 15 del Codice della Privacy stabiliva che chiunque cagiona un danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento se non prova di aver adottato tutte le misure idonee ad evitare il danno (art. 2050 c.c.). Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11 (Modalità del trattamento e requisiti dei dati). Questa disposizione è ora abrogata dal D.L. 101/2018. Poiché nella riforma nulla è previsto in tema di responsabilità civile e manca anche ogni richiamo all'art. 2050 Cod. Civ., la norma di riferimento in tale ambito diviene esclusivamente l'art. 82 del Reg. UE 679/2016, articolo che sancisce il diritto di chiunque di ottenere il risarcimento del danno subito a fronte di ogni violazione delle disposizioni del GDPR ad opera del titolare o del responsabile del trattamento (e non più "chiunque" avesse cagionato il danno). La normativa UE conferma gli obblighi risarcitori del danno materiale o immateriale in capo al titolare del trattamento che non ha rispettato il Regolamento ma lo esonera dalla responsabilità ove dimostri che l'evento dannoso non è in alcun modo a lui imputabile. Sono introdotte, poi, ipotesi di responsabilità solidale per l'intero ammontare del risarcimento in caso di più titolari o responsabili ed è previsto il diritto di rivalsa su ognuno in caso di pagamento per intero da parte di un solo soggetto[21].

[19]R. Motroni, Dati personali, rapporti economici e mercati finanziari, Cacucci, 2017, pagg. 15 ss.

[20]"Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno", art. 2050 C.C.

[21] Cfr. Senato Della Repubblica, Dossier "L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679" 21 maggio 2018, https://www.senato.it/service/PDF/PDFServer/BGT/01067350.pdf

Sulla base di quanto sopraesposto, è interessante approfondire la disciplina oggi in vigore, con particolare riferimento ai temi dell'inversione dell'onere probatorio e della solidarietà.

Come visto, tramite il D. Lgs. 101/2018, il legislatore ha previsto l'abrogazione del summenzionato art. 15 e l'art. 82 GDPR ora in vigore, nel confermare la possibilità per qualunque soggetto di avanzare richiesta di risarcimento, limita il corrispondente obbligo risarcitorio ai soli soggetti di cui all'art. 4, n. 7 e 8. Permane inoltre invariata la natura non solo patrimoniale ma anche non patrimoniale per cui il risarcimento potrà richiedersi.

Un tema di particolare interesse riguarda, come anticipato, l'inversione dell'onere della prova.

In tal senso, l'art. 82, in linea con quanto summenzionato e già contemplato dall'art. 15 D. Lgs. 196/2003, pone in capo al titolare ed al responsabile del trattamento che intendano esonerarsi da responsabilità l'onere di provare di non essere imputabile rispetto al fatto dannoso, prova che potrà avvenire ove si dimostri o che l'evento dannoso è derivato da una causa estranea alla propria sfera di controllo oppure l'adeguatezza delle misure predisposte.

La ratio a sostegno dell'inversione probatoria può riscontrarsi nella natura pericolosa delle operazioni di trattamento dei dati, le quali comportano un rischio per i soggetti coinvolti. Ferma infatti l'accettazione giuridica di tale rischio in considerazione dell'inevitabilità e dei vantaggi del trattamento dei dati, in particolare sotto i profili sociale ed economico, è pur vero che tali aspetti non esonerano il legislatore dalla necessaria tutela di eventuali soggetti danneggiati.

Conseguentemente, mentre in capo al titolare ed al responsabile del trattamento pende l'onere di provare la propria totale estraneità rispetto al fatto dannoso, 3 soli elementi dovranno essere oggetto di prova da parte del danneggiato: l'infrazione della norma sulla protezione dei dati personali, il verificarsi del danno ed il rapporto causale tra i 2 aspetti.

Un ulteriore tema di significativo interesse è quello della solidarietà. Allo scopo di tutelare il diritto del danneggiato al risarcimento, la normativa UE ha sancito il regime della responsabilità solidale, per cui, in ipotesi più soggetti di cui all'art. art. 4, n. 7 – 8, Reg. 679/2016, siano coinvolti nel medesimo trattamento e responsabili dell'eventuale evento dannoso, ciascuno di essi sia responsabile in solido per il l'importo complessivo del danno. Correlativamente, è riconosciuta in capo ai medesimi soggetti la facoltà di convenire in giudizio gli eventuali titolari o responsabili inadempienti tramite azione di regresso, allo scopo di conseguire la percentuale di risarcimento loro spettante.

Dunque, per effetto del regime di responsabilità solidale, il soggetto danneggiato potrà avanzare richiesta di risarcimento nei confronti tanto del titolare quanto del responsabile coinvolti, non essendo necessaria un'indagine volta a definire i differenti gradi di responsabilità.

In tema di solidarietà, pur se in senso lato, può farsi un rapido riferimento al dettato dell'art. 26 Reg. 679/2016, che disciplina l'ipotesi in cui 2 o più titolari del trattamento determinino congiuntamente le finalità ed i mezzi dello stesso, qualificandoli come "contitolari del trattamento". La norma si limita però ad indicare la necessità di definire le rispettive responsabilità con trasparenza e tramite un accordo interno, omettendo di chiarire cosa debba intendersi per "determinazione congiunta".

In tal senso, può analizzarsi la giurisprudenza della Corte di Giustizia UE, la quale, nel caso Wirtschaftsakademie Schleswig-Holstein (C-210/16), ha statuito come il creatore di una fan page sul social network Facebook fosse contitolare del trattamento dei dati interessati (tale soggetto poteva infatti non solo consentire il download di cookies sui dispositivi degli utenti, ma anche acquisire i loro dati demografici, di preferenze di acquisto, …) insieme a Facebook Ireland Ltd.

In una differente fattispecie, Jehovan Todistajat (C-25/17), la Corte ha ritenuto una comunità religiosa, i Testimoni di Geova finlandesi, responsabile del trattamento, insieme ai propri membri predicatori, di dati personali raccolti da questi ultimi nell'ambito di un'attività di predicazione porta a porta. Condizione sufficiente a tal fine è la mera organizzazione, coordinazione ed incoraggiamento da parte della comunità, a prescindere che la stessa abbia poi effettivo accesso ai dati[22].

È possibile dunque sostenere come la Corte avalli un'interpretazione tendenzialmente estensiva della nozione di "determinazione congiunta".

Fermo tale aspetto, a conclusione dei giudizi di risarcimento, ciascun titolare e responsabile sarà tenuto a rispondere per la rispettiva percentuale di responsabilità, per cui il regime di responsabilità che verrà a prefigurarsi sul lato interno sarà "pro quota" secondo le regole generali.

È opportuno peraltro sottolineare come il tema della responsabilità civile non si limiti all'infrazione delle disposizioni di cui sopra. Occorre infatti ricordare che il rapporto tra titolare e responsabile è disciplinato da un contratto, o da altro atto giuridico, secondo il diritto dell'Unione o degli Stati membri, il quale peraltro regolamenta ulteriori elementi quali, a titolo di esempio, durata e scopo del trattamento, tipologia di dati trattati e situazioni giuridiche attive e passive in capo alle parti.

Nel rapporto tra titolare e responsabile, l'atto giuridico in questione vincolerà il secondo non solo all'osservanza di quanto disposto dal primo, ma anche a fornire a quest'ultimo ogni informazione per provare l'ottemperanza al dettato dell'art. 28 GDPR, consentendo e coadiuvando le operazioni di revisione (es.: ispezione) ed a comunicare tempestivamente al medesimo la propria convinzione che una data istruzione contrasti con la normativa, UE o degli Stati membri, sulla tutela dei dati. Quanto esposto

[22] Per approfondimenti vd. Ivana Nemceková, Liability of Joint Controllers in the light of the CJEU Case Law, in EuroCloud – Trusted Digital, Competence Platform, 26 febbraio 2019

suggerisce una responsabilità decisamente più estesa in capo al responsabile del trattamento, mentre a carico del titolare si prefigura un duplice obbligo: la selezione dei responsabili e la vigilanza sulla loro condotta.

Per quanto attiene alla responsabilità per violazione degli obblighi sulla tutela dei dati, occorre poi segnalare come essa permanga in capo al titolare del trattamento, il quale non potrà in alcun caso demandarla a soggetti terzi.

Sino a questo momento si è trattato del danno prescindendo dalla natura di quest'ultimo. Per effetto di un trattamento di dati personali possono infatti determinarsi danni di carattere tanto patrimoniale quanto non patrimoniale, anche se, in considerazione della tipologia di interessi coinvolti, è frequente che l'evento dannoso emerga nella propria componente non patrimoniale.

Una rapidissima ricognizione storica sull'evoluzione del concetto (e della sua prova) lascia intendere come il tema del danno non patrimoniale sia stato, almeno negli ultimi decenni, tanto strettamente correlato alla condizione politica ed economica nazionale da rappresentare uno degli ambiti del diritto civile più dibattuti tra dottrina e giurisprudenza.

Punto di partenza, solo accennato, possono essere le pronunce della Corte Costituzionale c.d. "Dell'Andro" (Sent. 184/1986) e "Mengoni" (Sent. 372/1994; Ord. 293/1996), le quali, in riferimento all'ambito sanitario, sostenevano rispettivamente l'identificazione del danno non patrimoniale con un "danno morale in senso stretto" e la ricomprensione del "danno biologico" nell'ambito dell'art. 2059 c.c.

Successivamente, è da evidenziarsi una riforma dell'interpretazione giurisprudenziale dell'art. 2059 tramite Cass. Civ., Sent. 8827/2003 e 8828/2003, e Corte Cost., Sent. 233/2003.

Tali pronunce hanno di fatto avallato una nuova impostazione per cui: i) il riferimento ai "casi determinati dalla legge" sarà da riferirsi non solo all'ambito penale (art. 185 c.p.) ma ai diritti inviolabili riconosciuti nel Testo Costituzionale; ii) il "danno biologico" dovrà ricomprendersi tra i "danni non patrimoniali", per cui esso troverà più specifica tutela nell'art. 2059 rispetto alla clausola generale dell'art. 2043; iii) il danno non patrimoniale sarà da qualificarsi in quanto danno-conseguenza, da allegarsi e dimostrarsi in giudizio anche tramite l'ausilio di valutazioni prognostiche e presunzioni.

Tra le statuizioni più rilevanti sono poi da segnalarsi Cass. Sez. Un., Sent. da 26972 a 26975/2008, le quali non hanno però dato seguito alle pronunce appena citate, omettendo di soddisfare le attese di chiarimento dell'operazione esegetica compiuta dalla Suprema Corte e dalla Consulta.

Il combinato disposto tra tali pronunce escludeva invece la classificazione del danno non patrimoniale in eterogenee sottocategorie, in particolare negando il riferimento al "danno esistenziale" in quanto suscettibile di ricondurre il danno non patrimoniale a quell'atipicità che caratterizza fattispecie escluse dall'ambito di applicazione della norma.

In tal senso, la Suprema Corte non riconosce la tutela risarcitoria, in quanto danno esistenziale, ad insoddisfazioni tipiche della vita quotidiana, limitando il risarcimento per danno non patrimoniale alle sole violazioni di diritti inviolabili dell'individuo costituzionalmente qualificati.

Sorvolando su ulteriori e più recenti pronunce, sembra opportuno qui soffermarsi su Cass. Civ., Ord. 14242/2018, la quale, sul tema specifico della tutela dei dati, sostiene l'obbligo automatico in capo al datore di lavoro di risarcire il danno non patrimoniale patito dal prestatore di lavoro qualora il primo non dimostri la previa adozione di ogni misura adeguata a scongiurare l'evento dannoso o ne provi l'inesistenza o comunque l'irrilevanza.

L'Ordinanza, la quale di fatto richiede ai fini del risarcimento che, insieme all'illiceità del trattamento, sussista anche la sensibile lesione della privacy, viene pronunciata nel giugno 2018, dunque è antecedente rispetto all'entrata in vigore del D. Lgs. 101/2018. Conseguentemente, essa prosegue nel richiamo dell'art. 15 del Codice della Privacy, ma certamente fornisce una chiara indicazione in merito alla strada perseguita dalla Suprema Corte.

Invero, nel nostro ordinamento le corti di ultima istanza ancora non hanno avuto occasione di esprimersi sul tema della tutela dei dati, e nello specifico della risarcibilità del danno non patrimoniale in tale ambito, successivamente all'entrata in vigore del D. Lgs. 101/2018.

Da segnalare sul punto è la sentenza del Tribunale di prima istanza di Diez (Germania) del 7 novembre 2018, prima (e ad oggi unica) pronuncia nel panorama giurisprudenziale degli Stati membri in materia di risarcibilità del danno non patrimoniale ai sensi dell'art. 82 GDPR23.

Nel caso di specie, l'attore chiedeva il risarcimento di euro 500,00 per la ricezione di un'e-mail in cui il convenuto chiedeva di inserire il primo in una newsletter, procedura qualificabile come "spam" secondo la normativa tedesca.

Il Tribunale escludeva però il diritto al risarcimento adducendo a sostegno un pagamento di euro 50,00 che il convenuto aveva già corrisposto all'attore a titolo di compensazione. In aggiunta ed a titolo accessorio, la Corte evidenziava come l'attore avesse ricevuto l'e-mail in data 25 maggio 2018, contestualmente all'inizio dell'applicazione del GDPR, con ciò suggerendo che l'illiceità della condotta convenuta potesse ritenersi temperata.

Da notarsi come il Tribunale di Diez abbia rigettato la richiesta attorea di applicazione dell'art. 267 TFUE e dunque omesso di sottoporre il caso alla giurisdizione della Corte di Giustizia UE24.

[23] Vd. Sentenza sul caso 8 C 130/18, 7 novembre 2018

[24] Per approfondimenti, vd. J. Spittka, Germany: First Court decision on claims for immaterial damages under GDPR, in Privacy matters – DLA's Piper Global Privacy & Data Protection, 12 dicembre 2018

Rimane aperto il problema della prova del danno non patrimoniale per cui, a più di un anno di distanza dall'inizio dell'applicazione del GDPR, ed a fronte della nomina di circa 500.000 Responsabili del trattamento, 7219 reclami presentati alle differenti Autorità per la privacy e 946 notifiche di violazioni dei dati, le sanzioni economiche irrogate ammontano a € 56.000.000, cifra considerevole ma da ridimensionarsi alla luce del fatto che € 50.000.000 provengono da un'unica sanzione, comminata dall'Autorità per la privacy francese (CNIL) a carico di Google[25].

Fermo l'indubbio risultato di aver conseguito una maggiore consapevolezza, nelle imprese e nella Pubblica Amministrazione, sulla necessità di tutelare i dati in proprio possesso, è opinione di chi scrive come il GDPR abbia molta strada dinanzi a sé, in particolare in termini d'implementazione. In tal senso si consideri come le aziende italiane, a fronte di investimenti milionari previsti per il 2018, non abbiano stanziato quasi alcun fondo di spesa in tema di privacy nel 2019, dato che suggerisce la diffusione dell'erronea convinzione per cui l'adozione, una sola volta, delle misure previste dal GDPR perduri nel tempo mantenendo per sempre la propria impresa o P.A. al riparo da sanzioni economiche e danni alla reputazione.
Per la disciplina processuale delle controversie sopraindicate è confermato il rito del lavoro, in accordo alle previsioni dell'art. 10 del decreto legislativo n. 150 del 2011, esse stesse oggetto di riforma[26].
Questa ultima previsione del GDPR in materia di regime probatorio si può considerare quindi come un'ennesima affermazione dell'interesse per la tutela dei diritti personali dimostrato dalla UE, in favore degli interessati, le persone fisiche ritenute parte debole dei contratti riguardanti il trattamento dei dati personali. Alla luce dello scenario non solo europeo, ma anche internazionale, in proposito, si auspica un sempre maggiore recepimento della normativa GDPR anche al di fuori delle ipotesi previste dal Regolamento stesso, adottando la disciplina UE come standard a cui uniformare il trattamento dati a livello mondiale. Inoltre, vista la particolare delicatezza e significatività dei dati, si auspica l'estensione del trattamento ai dati delle persone giuridiche, del resto già riconosciute come titolari di diritti della personalità.
Nella inattività delle istituzioni (fino ad ora), è significativo constatare come talune imprese si siano già mosse in tal senso, adottando *policies* conformi al GDPR sia per il trattamento dei dati di soggetti extra UE, sia per il trattamento dei dati di persone giuridiche.

[25] Cfr. M. Martorana, GDPR: prime valutazioni a un anno dall'entrata in vigore, in Altalex, 21/06/2019
[26] Cfr. Senato Della Repubblica, Dossier "L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679" 21 maggio 2018,
https://www.senato.it/service/PDF/PDFServer/BGT/01067350.pdf