Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

ANGELA BUSACCA*

LE "CATEGORIE PARTICOLARI DI DATI" EX ART. 9 GDPR
*DIVIETI, ECCEZIONI E LIMITI ALLE ATTIVITÀ DI TRATTAMENTO***

SOMMARIO: 1. Circolazione dei dati e (necessità di una) tutela multilivello. - 2. Nuove dimensioni della privacy europea: i principi del GDPR. - 3. Dati personali e "categorie particolari" di dati personali. - 4. Tra proprietà ed accesso: le "categorie particolari di dati personali" come (necessario) punto di partenza per una rinnovata strategia di *data protection on line*.

1. *Circolazione dei dati e (necessità di una) tutela multilivello*

Sono già trascorsi più di diciotto mesi dalla data di entrata in vigore del Regolamento 679/2016, cd. "*general data protection*"[1] (cioè il 25 maggio 2016) e mancano ormai pochi mesi

* Ricercatrice di Diritto privato, Università Mediterranea di Reggio Calabria.

** Il presente testo, ripropone, con alcune modifiche e l'aggiunta dell'apparato di note, alcune parti del testo dell'intervento presentato in occasione del Convegno "Nuove tecnologie e diritti umani: profili di diritto internazionale e di diritto interno", organizzato dal Dipartimento di Giurisprudenza "Salvatore Pugliatti" e dal Dipartimento di Scienze Politiche e Giuridiche dell'Università di Messina nei giorni 26/27 Maggio 2017.

[1] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"; il testo integrale è consultabile, in tutte le lingue dei Paesi dell'Unione, sub http://eur-lex.europa.eu.
Nell'ambito della bibliografia italiana sul Regolamento possono, sin d'ora, segnalarsi S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy*, Padova, 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati. I) Dalla Direttiva 95/46 al nuovo Regolamento europeo. II) Il regolamento europeo 2016/679*, Torino, 2016; C. BISTOLFI, L. BOLOGNINO, E. PELINO, *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali,* Milano, 2016; M. MAGLI, M. POLINI, N. TILLI (a cura di), *Manuale di diritto alla protezione dei dati personali. La privacy dopo il Regolamento UE 2016/679*, Santa'Arcangelo di Romagna, 2017; N. BERNARDI, A. MESSINA, *Privacy e Regolamento Europeo*, Milano, 2017; V. CUFFARO, F. DI CIOMMO, R. D'ORAZIO, A. MANTELERO, M. L. GAMBINI, *Trattamento dei dati personali e Regolamento UE n. 2016/679*, e.book

alla data indicata come *deadline* per l'applicazione dello stesso ed il conseguente allineamento tra la normativa nazionale ed il contenuto del Regolamento: entro il 25 maggio 2018, come da previsione dell'art. 99[2], infatti, la regolamentazione nazionale, attualmente contenuta nel d.lgs.196/2003 (cd. Codice della Privacy[3]) dovrà adeguarsi per garantire l'uniformità del quadro normativo in materia di tutela delle persone fisiche con riferimento al trattamento dei dati personali[4], passando dall'approccio statico che caratterizzava l'impianto della Direttiva 95/46/CE ad un metodo più dinamico[5], configurato sulla scorta della realtà dei nuovi canali di comunicazione e dei flussi di

speciale di "Corriere giuridico"; G. FINOCCHIARO, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *NLCC*, 2017, 1 ss; F. PIRAINO, *Il regolamento generale sulla protezione dei dati ed i diritti dell'interessat*o, in *NGCC*, 2017, p. 369 ss.; M.G. STANZIONE, *Il regolamento europeo sulla privacy: origine ed ambito di applicazione*, in *Europa e Diritto Privato*, 2016, p. 1249 ss.

[2] L'art. 99 del Regolamento prevede, al comma 1, l'entrata in vigore a decorrere dal ventesimo giorno dalla pubblicazione nella *Gazzetta Ufficiale dell'Unione Europea*, ed al comma 2, che "esso si applica a decorrere dal 25 maggio 2018", offrendo così agli Stati membri un ampio margine di tempo per prepararsi al nuovo modello di privacy proposto dal Regolamento che "costituisce una occasione per una riflessione sistematica sulla filosofia, prima ancora che sulla disciplina della materia" (in questi termini SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy,* cit., p. 1).

[3] Nell'ambito della vasta bibliografia sul d.lgs. 196/2003 (cd. Codice Privacy), cfr. G. FINOCCHIARO, *Privacy e protezione dei dati personali. Strumenti operativi*, Bologna 2012; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, *Il codice del trattamento dei dati personali*, Torino, 2007; F. BERGADANO, A. MATELERO, G. RUFFO, G. SARTOR, *Privacy digitale. Giuristi ed informatici a confronto*, Torino, 2005; AA.VV., *Il Codice della Privacy,* Milano, 2004; R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003.

[4] In argomento, si consideri quanto espressamente indicato in incipit dal Considerando n.10 : "Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione"; peraltro già il precedente Considerando n.9 aveva evidenziato la frammentazione del quadro regolamentare all'interno dell'Unione a seguito del recepimento della Direttiva 95/46/CE, affermando che sebbene debbano considerarsi validi obiettivi e principi della citata Direttiva, tuttavia proprio la frammentazione e le differenze derivate dai diversi livelli di tutela rinvenibili negli Stati membri, finiscano per determinare "l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche", con la conseguenza che "la compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione" e determinare situazioni di freno all'esercizio di attività economiche transnazionali su scala europea.

[5] In questo senso G. FINOCCHIARO (*Introduzione al regolamento europeo, cit*.,1) sottolinea come la Direttiva 95/46/CE "aveva recepito un dibattito culturale e un pensiero dottrinale sviluppatosi nei decenni precedenti e delineato un modello statico di trattamento dei dati personali, ormai superato" che rispondeva alle esigenze di "un mondo privo di smartphone, social network e motori di ricerca"; diversamente la realtà attuale che l'autrice definisce con significativa immagine come "un mondo digitalmente sempre interconnesso", si basa non più su flussi di dati monodirezionali, ma piuttosto sulla circolazione, multilivello e multidirezionale, di flussi di dati in condivisione e cogestione, "destinati fin dall'origine ad una circolazione globale".

informazione circolari che caratterizzano il web 2.0[6], nonché delle capacità pervasive dei motori di ricerca[7] e della necessità di una tutela multilivello in grado di coniugare e garantire protezione non soltanto ai diritti soggettivi tradizionali, ma anche e soprattutto ai cd. diritti "nativi", ontologicamente connaturati all'ecosistema Internet[8].

In particolare, con riferimento alle informazioni ed ai dati personali, appare non più esaustiva la bipartizione tra "diritto alla riservatezza" e "diritto alla tutela dei dati

[6] L'espressione web 2.0 viene comunemente utilizzata per indicare la fase di sviluppo della Rete Internet caratterizzata dalla possibilità di interazione e modifica delle pagine web e dei flussi di informazione da parte degli utenti; la maggiore interazione e la realizzazione di flussi di informazione multidirezionali coinvolgono in misura sempre maggiore gli utenti della Rete che possono diventare (anche) coproduttori dei contenuti veicolati. In questo senso si moltiplica la presenza in Rete degli UGC (*user generated content*), creati dagli stessi internauti/utilizzatori non professionisti ed immessi con operazioni di upload; parallelamente, la diffusione dei dispositivi mobili determina la moltiplicazione esponenziale delle modalità e delle occasioni di circolazione e condivisione delle informazioni; in argomento sintetizzano efficacemente S. FARO, N. LETTIERI (*Big Data e Internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della Rete*, in L. RUGGERI, C. PERLINGIERI (a cura di), *Internet e diritto civile*, Napoli, 2015, 279): "la varietà dei dati elettronici relativi a ciascuno di noi è notevolmente aumentata, in parte a causa della comparsa dei social media e in parte a causa della crescita dei dispositivi mobili, dei dispositivi di sorveglianza e di una varietà si sensori collegati in Rete (…) molto spesso, senza esserne a conoscenza, gli individui producono costantemente informazioni, che vengono raccolte, conservate e frequentemente usate per finalità diverse da quelle per cui esse sono state originariamente raccolte", sottolineando poi come il modello di tutela statico, proprio del web 1.0 e modellato sui cd. "small data" appare del tutto inadeguato per i Big Data propri del web 2.0.
In argomento cfr. altresì A. PARAFIORITI, *The Big Data e la conoscenza nella società del web 2.0*, Roma, 2014; con ottica rivolta alla dinamica dell'e.commerce, F. DELLA VOLPE, *Imprese tra web 2.0 e Big Data*, Padova, 2013 (spec. *cap. I: L'evoluzione del web: un'analisi di scenario*).

[7] I. DEL MARCO, V. PEZZINI, *Nella Rete di Google. Pratiche strategie e dispositivi del motore di ricerca che ha cambiato le nostre vite*, Milano, 2017; con approccio tecnico, M. MELUCCI, *Information Retrieval. Metodi e modelli per i motori di ricerca*, ebook, Milano, 2016. Con riferimento ad alcune questioni giurisprudenziali, prime fra tutte la de-indicizzaione e la tutela della riservatezza e del diritto all'oblio, cfr. F. MELIS, *Il diritto all'oblio e i motori di ricerca nel diritto europeo*, in *Giornale di diritto amministrativo*, 2015, 171 ss.; L. BUGIOLACCHI, *Quale responsabilità per il motore di ricerca in caso di mancata deindicizzazione su legittima richiesta dell'interessato?*, in *Resp civ prev*, 2016, p. 571 ss.; E. TOSI, *Contrasti giurisprudenziali in materia di responsabilità civile degli "hosting provider" - passivi e attivi - tra tipizzazione normativa e interpretazione evolutiva applicata alle nuove figure soggettive dei motori di ricerca, "social network" e aggregato*, in *Rivista di diritto industriale*, 2017, p. 75 ss.; F. VISCO COMANDINI, *Google e i mercati dei servizi di ricerca su Internet*, in *Mercato concorrenza regole*, 2013, p. 541 ss.

[8] La categoria dei diritti cd. "nativi" individua tutte quelle situazioni soggettive correlate alle proiezioni della persona nella dimensione Internet, che non possono né devono considerarsi come semplici declinazioni delle tradizionali figure di diritti della personalità; seppur in un primo momento, infatti, l'opera della giurisprudenza si era indirizzata alla tutela delle tradizionali figure dei diritti della personalità, non cogliendo le caratteristiche dell'ambiente Internet, tuttavia proprio lo sviluppo della Rete ha reso necessaria una presa di coscienza sull'emersione ed affermazione di tutta una serie di nuove situazioni giuridiche da considerarsi come situazioni a rilevanza autonoma, con proprie caratteristiche derivate essenzialmente dall'ecosistema Internet e relate alle peculiarità del contesto virtuale: si tratta di diritti che vengono spesso indicati come "di quarta generazione" e che, sebbene di emersione giurisprudenziale, hanno trovato anche alcuni (sebbene) sporadici riconoscimenti normativi in ambito europeo. In argomento, cfr. G. DE MINICO, *Antiche libertà e nuove frontiere digitali*, Torino, 2016 (spec. p. 44 ss); L. MASERA- G. SCORZA, *Internet, I nostri diritti*, Roma-Bari, 2016; FEMIA, *Una finestra sul cortile. Internet e il diritto all'esperienza metastrutturale.* in L. RUGGERI, C. PERLINGIERI (a cura di), *Internet e diritto civile*, cit., p. 15 ss; G. FINOCCHIARO, *I diritti della personalità in Rete*, in G. FINOCCHIARO, F. DELFINI, *Diritto dell'Informatica*, Torino, 2014; D. BIANCHI, *Internet e il danno alla persona*, Torino, 2012.

personali"[9], dovendo considerarsi altresì la "*data protection on line*" ed il diritto all'oblio[10], la tutela contro le attività di *spoofing*, *profiling* e di *phishing*[11], la tutela dell'identità digitale[12],

[9] G. PASCUZZI, F. GIOVANNELLA, *Dal diritto alla riservatezza alla computer privacy*, in G. PASCUZZI (a cura di), *Il diritto dell'era digitale*, Bologna, 2016, 43 ss; la bipartizione tra diritto alla riservatezza e diritto al trattamento dei dati personali viene analizzata da G. FINOCCHIARO (*Introduzione al Regolamento europeo sulla protezione dei dati, cit.*, 2 ss) con riferimento alle situazioni previste e tutelate dalla Convenzione Europea dei Diritti dell'uomo: l'autrice, infatti, sottolinea come il diritto alla protezione dei dati personali sia contemplato all'art. 8 CEDU nell'ambito dei diritti di libertà, come diritto di ciascun individuo alla protezione dei dati di carattere personale che lo riguardano e come diritto ad un trattamento dei dati che sia effettuato secondo i principi di lealtà, finalità e proporzionalità; parimenti il diritto alla protezione della vita privata e della vita familiare , ai quali si riporta il tradizionale concetto di privacy come *right to be left alone*, viene contemplato all'art. 7. Sul portato delle differenti situazioni giuridiche di riferimento, l'autrice afferma che "il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per questa ragione è frequente che il diritto alla protezione dei dati personali sia inteso come diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi".

[10] L. GATT, R. MONTANARI, I. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale*, in D. POLETTI, P. PASSAGLIA (a cura di), *Nodi virtuali, legami informali. Internet alla ricerca di regole,* Pisa, 2017, p. 57 ss.; G. DI GENIO, *Trasparenza ed accesso dati personali,* in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy,* cit., 161; V. D'ANTONIO, *Oblio e cancellazione dei dai nel diritto europeo, ivi,* p. 197 ss. In tema di diritto all'oblio, cfr. S. MARTINELLI, *Diritto all'oblio e motori di ricerca*, Milano, 2017; M. TAMPIERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Responsabilità civile e previdenza*, 2017, p. 1010 ss.; G. M. RICCIO, *L'esordio del diritto all'oblio nella giurisprudenza italiana* in *Il Diritto dell'informazione e dell'informatica*, 2016, p. 271 ss.; ID., *Il difficile bilanciamento tra diritto all'oblio e diritto di cronaca*, in *NGCC*, 2017, p. 549; F. DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, in *Danno e Responsabilità,* 2014, p. 1101 ss.; T. E. FROSINI, *Google e il diritto all'oblio preso sul serio,* in *Diritto informazione e informatica*, 2014, p. 563; G. G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità, ivi* , p. 591.

[11] *Spoofing, profiling e phishing* rappresentano tre dei più ricorrenti illeciti realizzati attraverso cyber-attacchi alla sicurezza della circolazione dei dati *on line* e condotte fraudolente di truffa ai danni dei soggetti proprietari dei dati; in particolare, lo *spoofing* indica, nella più estrema semplificazione, una manipolazione dei dati con falsificazione di identità ed utilizzo abusivo di credenziali di accesso e dati personali carpiti ad altri utenti; il termine *profiling*, invece, indica la tracciatura (illecita) della navigazione con finalità di ricostruzione della personalità e dell'identità digitale del soggetto e, anche in questo caso, manipolazione dei dati personali; da ultimo, il phishing rappresenta la fraudolenta acquisizione dei dati attraverso invio di false comunicazioni od in commistione con attività di *social engineering*, al fine di ottenere credenziali di accesso a sistemi o servizi dell'interessato per poter, poi, sostituirsi e realizzare transazioni ed operazioni varie on line. Sul tema, con particolare attenzione ai profili di responsabilità collegati, cfr. D. BIANCHI, *Internet e il danno alla persona, cit.* (spec. Cap.VII, 163 ss) ; A. VALORE, *Phishing sul conto postale e trattamento dei dati* in *Corriere del merito*, 2012, 663; T. FANTINI, *Phishing: strategie operative dell'inganno,* in *Il diritto dell'Internet*, 2008, 421.

12 In argomento, cfr. G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e Impresa,* 2017, 723 ss.; S. LANDINI, *Identità digitale tra tutela della persona e proprietà intellettuale* in *Diritto industriale*, 2017, 180 ss.; L. TRUCCO, *Identificazione e anonimato in rete*, in D. POLETTI, P. PASSAGLIA (a cura di), *Nodi virtuali, legami informali. Internet alla ricerca di regole,*cit., 281 ss.; M.F. COCUCCIO, *Il diritto all'identità personale e l'identità "digita*le", in *Il Diritto di famiglia e delle persone*, 2016, 949 ss.; A. O. ROVEGNO, *Identità digitale: tra esigenze di condivisione e necessità di tutela,* in *Ciberspazio e Diritto*, 2013 403 ss; M. BRUGI, *Dall'identità personale all'identità digitale. Una necessità per il cittadino del terzo millenn*io, in *Informatica e diritto*, 2008, 167 ss.

nonché le diverse dimensioni della tutela nella circolazione dei dati correlati alle attività e-commerce[13].

Come emerge dalla lettura dei considerando premessi al Regolamento (ben 173 considerano a fronte di 99 disposizioni dell'articolato normativo) ed in particolare dal Considerando n. 9[14], la frammentazione del composito quadro normativo attuale, come risultante dalle singole legislazioni nazionali, ha determinato non soltanto un senso di incertezza giuridica, ma altresì una diffusa percezione di rischio per le operazioni on line, financo di diffidenza per tutte quelle operazioni che, sia nell'area delle comunicazioni che in quella delle transazioni e.commerce, importavano il trasferimento di dati personali in ambito continentale (e spesso anche oltre i confini europei[15]).

2. *Nuove dimensioni della privacy europea: i principi del GDPR*

Con il Regolamento 679/2016 il legislatore europeo opta decisamente per un innalzamento, qualitativo e quantitativo, delle soglie di tutela, scegliendo uno strumento di unificazione (e non più di armonizzazione) e ponendolo nel quadro di più generale rinnovamento normativo: accanto al Regolamento "*General Data Protection*", possono infatti considerarsi il Regolamento 910/2014 cd. e.IDAS (*Electonic Identification, Authentication,*

[13] In argomento cfr. A. PARISI, *E-contract e privacy*, Torino, 2016; in relazione al valore dei dati personali nell'economia delle transazioni on line e delle attività di web marketing, cfr. M. MAGLIO, *Il valore economico dei dati personali: spunti per un'analisi economica della data protection*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali,* cit.*,* p. 79 ss, nonchè ID., *Dati personali, attività di marketing e riutilizzo delle informazioni, ivi,* p. 631 ss.

[14] Il Considerando n. 9 recita testualmente "Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE"; appare chiaro come la scelta del Regolamento sia, su queste premesse, la migliore proprio nell'ottica di una unificazione in grado di assicurare un elevato livello di tutela (sul punto cfr. M. G. STANZIONE, *Il regolamento europeo sulla privacy: origini ed ambito di applicazione, cit.*, p. 1249 ss.)

[15] Proprio con riferimento alla circolazione transfrontaliera dei dati, ed in particolare alla circolazione verso paesi terzi, sul portato dei considerando n.6 e n.101 (che evidenziano l'importanza dei flussi di dati verso e da paesi extra UE ed organizzazioni internazionali, sia per finalità di cooperazione internazionale che di commercio internazionale), l'intero Titolo V del Regolamento è dedicato al "Trasferimento di dati personali verso Paesi Terzi o Organizzazioni internazionali", individuando i profili di differenza tra attività di comunicazione ed attività di trasferimento; sul punto, cfr. D. PITTELLA*, Trasferimento verso paesi terzi,* in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy*, cit., p. 259.

signature)[16] e la Direttiva 2016/680/UE relativa al "trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati"[17].

Il cd. "pacchetto protezione dati"[18], nelle intenzioni del legislatore europeo, rappresenta dunque una priorità, anche e soprattutto in considerazione delle più recenti pronunce della Corte di Giustizia Europea che, dal caso Digital Ireland fino al cd. Caso Schrems[19] e passando per la storica sentenza Costeja (nota come caso Google Spain[20]), avevano evidenziato la necessità di una serie di innovazioni, rispetto all'impianto classico

---

[16] M. TESCARO, *Le regole di responsabilità del Regolamento 'eIDAS,* in *NLCC*, 2017, 542 ss.; G. FINOCCHIARO, *Una prima lettura del Reg. UE n. 910/2014 (c.d. "Eidas"): identificazione "on line", firme elettroniche e servizi fiduciari (reg. UE n. 910/2014)*, *ivi*, 2015, p. 419 ss.

In relazione al tema dei sistemi di identificazione, con riferimento all'esperienza italiana di SPID (sistema pubblico di identità digitale), cfr. A. CONTALDO, *La disciplina dello SPID e la definizione giuridica dei suoi gestori*, in *Rivista Amministrativa della Repubblica Italiana*, 2016, p. 541 ss; L. ABBA, V. AMENTA, L. LAZZARONI, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al "web"*, in *Ciberspazio e Diritto*, 2015, p. 11 ss.

[17] I. MARIOTTINI, *Il pacchetto di riforma della Commissione europea in materia di protezione dei dati personali*, in *Riv. dir. int. priv. proc.*, 2016, p. 905 ss.; M. FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali*, in *Diritto comunitario e degli scambi internazionali*, 2016, p. 1 ss.

[18] L'espressione è utilizzata anche da M. BASSINI, *La "svolta" della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quaderni costituzionali*, 2016, 587 ss.

[19] Le sentenze della Corte di Giustizia (Grande Sezione) datate 8 aprile 2014 (*Digital Rights Ireland Ltd* contro *Minister for Communications, Marine and Natural Resources e a.* e *Kärntner Landesregierung e a.*) e 6 ottobre 2015 (*Schrems c. Data protection Commissioner Ireland*) rappresentano i leading case in tema di affermazione di un nuovo paradigma di tutela dei dati personali. Nell'ambito della vasta bibliografia in argomento, si possono segnalare, G. RESTA, V. ZENO ZENCOVICH (a cura di), *La protezione transnazionale dei dati. Dal "Safe Harbour" al "Privacy Shield"*, e.book, Roma, 2016; L. GRECO, L. VALLE, *Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale,* in *Il Diritto dell'informazione e dell'informatica*, 2017, p. 169 ss.; B. CAROTTI, *La Corte di Giustizia costruisce un ponte tra riservatezza e comunicazioni elettroniche* in *Giornale di diritto amministrativo*, 2017, p. 479 ss.; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal "Safe Harbour" al "Privacy Shield")*, in *Riv. dir. int*, 2016, p. 690 ss.; A. MANTELERO, *From "Safe Harbour" to "Privacy Shield". The "medieval" sovereignty on personal data*, in *Contratto e impresa. Europa*, 2016, p. 338 ss.; A. GIATTINI, *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso "Schrems" e l'invalidità del sistema di "approdo sicuro"*, in *Dir. um. dir. int.*, 2016, p. 247 ss.; V. ZENO ZENCOVICH, *Intorno alla decisione nel caso "Schrems": la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* in *Il Diritto dell'informazione e dell'informatica*, 2015, p. 683 ss.

[20] Nell'ambito della vasta bibliografia sviluppatasi dopo la storica sentenza della Corte di Giustizia Europea, 13 maggio 2014, c-141/12 (cd. caso *Costeja*), cfr. F. MELIS, *Il diritto all'oblio e i motori di ricerca nel diritto europeo,* in *Giornale di diritto amministrativo*, 2015, 71 ss.; F. DI CIOMMO, *Quello che il diritto non dice. Internet e oblio*, in *Danno e Responsabilità,* 2014, p. 1101 ss.; T. E. FROSINI, *Google e il diritto all'oblio preso sul serio,* in *Diritto informazione e informatica*, 2014, 563; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità, ivi*, p. 591; O. POLLICINO, *Un "digital right to privacy" preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel "reasoning" di "Google Spain*", in *Il Diritto dell'informazione e dell'informatica*, 2014, p. 569 ss.; A. MANTELERO, *Il futuro regolamento EU sui dati personali e la valenza "politica" del caso "Google": ricordare e dimenticare nella "digital economy*", in *Il Diritto dell'informazione e dell'informatica*, 2014, p. 681 ss.; F. PIZZETTI, *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di Giustizia sul caso "Google Spain": è tempo di far cadere il "velo di Maya", ivi*, 2014, p. 805 ss; G. E. VIGEVANI, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano,* in *Danno e responsabilità*, 2014, p. 742 ss.

della tutela dei dati, come emergente dalla normativa di derivazione dalla Direttiva 95/46/Ce.

Il nuovo approccio si basa, nelle sue linee generali, su una più dinamica considerazione dei flussi di dati, sul principio di *accountability* (termine utilizzato nel linguaggio economico che presenta qualche difficoltà di traduzione nel lessico delle nostre categorie giuridiche, tanto da indurre alcuni dei primi commentatori a preferire il termine anglosassone proprio per mantenere le caratteristiche delle situazioni incombenti sul titolare e sul responsabile del trattamento[21]), nonché sulla valutazione dei rischi che possono derivare dalle attività di trattamento[22], con un decisivo passaggio all'approccio precauzionale[23].

---

[21] Sul principio di *accountability*, cfr. G. FINOCCHIARO (*Introduzione al regolamento europeo sulla protezione dei dati, cit.*, 11 ss) la quale evidenzia come il termine posa essere tradotto con "responsabilità" ed al contempo "prova della responsabilità"; il principio in questione può rintracciarsi nell'art.32 che pone in capo al titolare del trattamento la valutazione in ordine alle misure tecniche ed organizzative da adottare, in relazione alla natura dei dati, all'oggetto ed alle finalità del trattamento. Come sottolineato, si determina una "visione integrata: informatica, giuridica ed organizzativa" che pongono come centrale il tema della sicurezza e le connesse responsabilità in caso di eventi patologici nelle attività di trattamento (distruzione, perdita, modifica, divulgazione non autorizzata, accesso non autorizzato o illegale). Del resto, posto che la sicurezza si atteggia come "concetto dinamico e relazionale, da rapportarsi alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati personali oggetto del trattamento ed alle specifiche operazioni di trattamento compiute", l'applicazione concreta del principio di *accountability* potrebbe rintracciarsi nella traduzione dei principi generali in tema di protezione dei dati in "politiche e procedure concrete definite al livello del responsabile del trattamento, nel rispetto delle leggi e dei regolamenti applicabili"

[22] In argomento, cfr. A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *NLCC*, 2017, p. 144 ss.; l'autore sottolinea che "proprio l'analisi dei rischi ed in conseguente processo di mitigazione di questi ultimi rappresentano la chiave di volta di un modello a venire, in cui la centralità dell'individuo e della sua tutela muovono da una dimensione endogena verso una dimensione esogena. Partendo infatti dall'assunto che gli individui non possono (…) essere completamente consapevoli delle potenziali conseguenze del trattamento dei dati in sistemi complessi, si deve approdare alla conclusione che tali conseguenze devono necessariamente e preventivamente valutate ad opera di terzi, in maniera per certi versi analoga a quanto accade per la sicurezza dei prodotti"; nell'ambito del Regolamento, peraltro, la valutazione dei rischi viene affrontata da una prospettiva multilivello con valutazioni poste a diversi livelli ed in ragione delle diverse modalità di trattamento che possono essere effettuate. Tuttavia, occorre sottolineare come parte della dottrina, come lo stesso autore, appaia piuttosto critica nei confronti della scelta del legislatore europeo, riconoscendo che, seppur costituisca una decisa innovazione, tuttavia l'approccio scelto appare rivolto ancora ad una tutela su base individuale, poco attenta alla dimensione collettiva ed agli ulteriori rischi determinati dalla gestione delle grandi masse di dati (sul punto, spec. 163-164)

[23] Al riguardo, vengono in considerazione principalmente gli artt. 25 e 35 del Regolamento, che pongono in capo al titolare l'obbligo di effettuare la valutazione di impatto (art.35) per quei trattamenti che possono presentare elevati rischi "per i diritti e le libertà" delle persone fisiche e che prevedono la predisposizione di strumenti di tutela "sin dalla progettazione" e "per impostazione predefinita"; si tratta di strumenti che determinano come evidenziato dalla dottrina, "un'impostazione al tempo stesso preventiva e promozionale della nuova normativa, volte ad attuare i principi operanti nel diritto europeo (…) un ruolo sempre più importante sembra essere svolto dai principi di prevenzione e di precauzione, allorché la normativa, pur non richiamandoli, discorre dei rischi aventi "probabilità e gravità diverse" per i diritti e le libertà delle persone interessate (art.25 reg.)o prevede l'obbligo della valutazione d'impatto quando il trattamento "può presentare" un rischio elevato per i diritti e le libertà delle persone fisiche" (in questi termini, M. G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, cit., 1249). Sul tema, cfr. altresì R. D'ORAZIO, *Protezione dei dati by default e by design*, in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della*

Ma l'innovazione riguarda anche i profili soggettivi ed oggettivi delle attività di trattamento dei dati: lasciando da parte i primi, con la considerazione delle figure del co-titolare e del *Data Protection Officer*[24]nonché la considerazione delle dinamiche relazionali tra gli stessi in caso di *data breach*[25], con riferimento ai profili oggettivi, la stessa nozione di "dato personale" contenuta all'art.4 del Regolamento subisce una riqualificazione qualitativa[26], e si arricchisce di alcune specificazioni in ordine a particolari categorie di dati[27]

---

privacy, cit., 79 ss; A. PRINCIPATO, *Verso nuovi approcci alla tutela della "privacy": "privacy by design" e "privacy by default settings"*, in *Contratto e impresa. Europa*, 2015, p. 197 ss.

[24] L'introduzione della figura del responsabile della protezione dati (RDP, più comunemente indicato con l'acronimo anglofono DPO, *Data Protection Officer*) è una delle più rilevanti novità del Regolamento; la nuova figura professionale, che non deve confondersi con il responsabile del trattamento, risulta finalizzata, in linea con il principio di *accountability*, a rafforzare la tutela e la sorveglianza nelle operazioni di trattamento dei dati, ponendosi come figura apicale e di interfaccia tra i soggetti a diverso titolo coinvolti nelle stesse attività di trattamento. In estrema sintesi, non essendo questa la sede per una disamina dei diversi profili relativi al DPO, appare sufficiente richiamare le linee generali degli artt. 37-39 del Regolamento che disciplinano le ipotesi di obbligatorietà della nomina (art. 37), la posizione ed i rapporti con i titolare (art. 38) ed i compiti e le funzioni (art. 39). Nel delineare i tratti caratterizzanti della nuova figura professionale, che risulta obbligatoria per le autorità pubbliche e gli organismi pubblici e per le società private che trattino notevoli moli di dati o che effettuino trattamenti su particolari categorie di dati (quali quelli contemplati all'art. 9), il Regolamento risulta, già ad una prima lettura, debitore della normativa tedesca del 2003 in tema di protezione dei dati (*Bundesdatenschutzgesetz*) che aveva già introdotto e reso obbligatoria la figura del *datenschutzbeauftrager* (DSB), in tutte le ipotesi di trattamento di dati sensibili o di attività che implichi trattamento svolta da un numero minimo di dipendenti (individuato in dieci qualora si utilizzino strumenti automatizzati o venti qualora si utilizzino strumenti manuali), sebbene questo abbia determinato, a detta già dei primi commentatori, una generale indeterminatezza nella specificazione dei compiti del DPO, con possibile aumento dei costi transattivi, a fronte di altre esperienze normative europee (ad es. quella spagnola). Sul punto cfr. G. M. RICCIO, *Data Protection Officer e altre figure*, in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy, cit*., p. 33 ss.; P. LAMBERT, *The Data Protection Officer: profession, rules and role*, CRC Press Boca Raton, 2017; N. BERNARDI, M. PEREGO, *Privacy Officer. La figura chiave della data protection europea*, Milano, 2017.

[25] La locuzione "*data breach*" può tradursi come "violazione dei dati personali" e ricorre, secondo quando indicato dall'art. 4 n. 12 del Regolamento, ogni qualvolta si verifichi una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"; si tratta, come appare evidente, di una fenomenologia vasta e complessa che richiama, al suo interno, non soltanto le ipotesi di violazione consapevole, ma altresì possibili ipotesi di violazione colposa o determinata da eventi non assistiti dalla volontà umana. In ogni caso, tra le innovazioni più significative del Regolamento, devono citarsi da un lato, la più efficiente procedura di notifica in caso di rilevazione di violazioni, e dall'altro, i rafforzati obblighi di sicurezza posti a carico dei soggetti che, a diverso titolo, dispongono e partecipano alle attività di trattamento. In argomento, cfr. S. VIGILAR, *Data Breach e sicurezza informativa*, in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy,* cit., p. 241; M. MAGLIO, *Cybersecutiry e dati personali,* in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali,* cit.*,* p. 719.

[26] Sul punto, evidenzia M. G. STANZIONE (*Il regolamento europeo sulla privacy: origini ed ambito di applicazione,* cit., p. 1256) come il Regolamento determini un significativo ampliamento dell'ambito di applicazione materiale, con l'estensione della nozione di "dato personale" a tutta una serie di informazioni che identificano o rendono identificabile la persona (nome, numero di identificazione, dati relativi alla geo-localizzazione, identificativi on line ed elementi relativi all'identità genetica). L'autrice sottolinea peraltro come "se non è possibile ridurre la persona ai suoi dati, sempre più questi sono indispensabili per il libero sviluppo della personalità", per rimarcare ulteriormente l'importanza del evoluzione della tutela dei dati personali, oltre le ambiguità che le definizioni della Direttiva 95/46/CE aveva determinato.

(indicate dal successivo art. 9 comma 1), per le quali vengono posti diversi livelli di tutela, anche e soprattutto in considerazione della diversa afferenza alla sfera sanitaria, esistenziale e relazionale del soggetto dei cui dati si tratta che mantiene la denominazione di "interessato"[28].

3. *Dati personali e "categorie particolari" di dati personali*

Punto di partenza per la nostra analisi, pertanto, non può che essere la definizione, di carattere generale di "dato personale", contenuta all'art. 4 n. 1 del Regolamento (ai fini del presente Regolamento, si intende per n.1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale) che deve essere confrontata con la precedente definizione contenuta nell'art. 2 della Direttiva 95/46/CE (Ai fini della presente direttiva si intende per «dati personali» qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale).

Già dalla prima lettura possono trarsi due considerazioni: da un lato permane la considerazione quasi sinonimica di "dato" ed "informazione" (il dato personale *è* qualsiasi informazione[29]), dall'altro appare manifesta l'attenzione allo sviluppo tecnico e

---

[27] La specificazione delle "categorie particolari di dati" concorre alla evoluzione qualitativa delle misure di tutela e protezione dei dati personali, posto che, come afferma M. GRANIERI (*Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679,* in *NGCC*, 2017, p. 166), "l categorie particolari di dati si inseriscono nel quadro complessivo di una disciplina che cerca al meglio di conciliare la tutela della persona fisica, riguardo alle informazioni sensibili che la riguardano, con l'esigenza che siano poste in essere attività rilevanti a livello economico e non (molte delle quali tipiche dello stato sociale e, dunque, rivolte a beneficio degli stessi cittadini dei cui dati si tratta), talora incidenti sulla ricerca scientifica, sulle prestazioni sanitarie e previdenziali, nonché su altre libertà fondamentali di chi svolge il trattamento".

[28] L'art. 1 nell'ambito delle molte definizioni rilevanti ai fini dell'applicazione del Regolamento, individua l'interessato come "una persona fisica identificata o identificabile", senza offrirne tuttavia una definizione autonoma, ma inquadrandolo nell'ambito della definizione di "dato personale" di cui al n.1; più in generale, anche in chiave critica sull'impianto del Regolamento (considerato come una disciplina sulla circolazione dei dati piuttosto che come disciplina di tutela della persona), cfr. F. PIRAINO, *Il Regolamento Generale sulla protezione dei dati personali e i diritti dell'interessato,* in *NLCC*, 2017, p. 371ss.

[29] Sul punto appare critica G. FINOCCHIARO (*Introduzione al Regolamento europeo sulla protezione dei dati, cit.,* 4) nell'affermare che "muovendo, dunque, dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che a questi si riferiscono" ed inoltre che "il diritto alla protezione dei dati personali è anche noto come "*information privacy*", "*informational privacy*", "*data privacy*", tutte espressioni nelle quali si evidenzia che l'oggetto del diritto è

tecnologico[30] che porta alla inclusione degli identificativi on line o geo-localizzanti ed altresì dei dati che possono portare alla identificazione genetica.

Proprio su queste ultime categorie, con riferimento agli identificativi on line, devono ritenersi compresi nel novero dei dati ex art.4 anche i cd. *recognition identifiers (R-identifiers)* e non più solo i *lookup identifiers (L-identifiers)*[31]: non solo, pertanto, i dati archiviati ed estraibili dalle banche dati o dalle memorizzazioni durevoli, ma anche i file di navigazione, i file temporanei ed altri dati "dinamici"[32] (peraltro talvolta già utilizzati con valore probatorio nell'ambito dei procedimenti di controllo a distanza da parte del datore di lavoro, con conseguente irrogazione di sanzione disciplinare[33]).

---

l'informazio-ne o il dato, benché a rigore dato e informazione siano termini non coincidenti". In argomento, cfr. altresì F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., p. 183 ss.

[30] Sulla necessità di implementare le strategie di tutela e di porre una regolamentazione più attenta agli sviluppi tecnologici del web 2.0 (ed in prospettiva del web 3.0), cfr. G. MARINI, *Diritto alla Privacy*, in *Commentario al Codice Civile* (a cura di E. GABRIELLI), *Delle Persone*. Vol. III. *Leggi collegate* (a cura di *Barba - Pagliantini*), Milano, 2013, p. 199 (ma spec. p. 246 ss., *Privacy e identità impigliati nella Rete*).

[31] In argomento cfr. M. GRANIERI (*Il trattamento di particolari categorie di dati personali nel reg. UE 2016/679,* cit., p. 169) il quale, in riferimento anche alle riflessioni di B. J. KOOPS (*The trouble with European Data Protection Law,* in *International Data Privacy Law,* 2014, p. 250 ss.) sottolinea come l'approccio della normativa europea fosse centrato sulla considerazione dei *lookupidentifiers,* cioè di tutti quei dati conservati ed archiviati in banche dati, schedari, registri e questi estratti (o estraibili) e che tale approccio finisca per risultare inadeguato in considerazione delle nuove possibilità tecnologiche di analisi, gestione, estrapolazione e combinazione di ingenti masse di dati, con l'impiego di processi automatizzati. A titolo esemplificativo basti citare il fenomeno della raccolta dei *cookies* di navigazione che permettono di estrapolare dati relativi non soltanto agli "itinerari" di navigazione degli utenti, ma altresì di ricavare dati che possono appartenere alle categorie di "dati sensibili" e rivelare profili riservati ed intimi della personalità (si pensi alle ideologie politiche od al sentimento religioso, od ancora ai dati inerenti lo stato di salute o le preferenze e l'orientamento sessuale); sui *cookies*, cfr. N. BUCCHERI, *Privacy e web*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali*, cit., p. 767 ss.

[32] Da ultimo, si consideri la sentenza della Corte Europea di Giustizia del 19 ottobre 2016, *Breyer c. Germania*, causa C-582, con la quale è stato ricondotto al novero dei dati personali anche l'indirizzo IP dinamico qualora il gestore del sito web visitato disponga di mezzi tecnici e giuridici per l'identificazione dei visitatori. Sul punto deve considerarsi che, mentre gli IP statici sono stati sempre pacificamente considerati dati personali (e quindi sottoposti all'operatività della direttiva europea), si ponevano alcuni dubbi con riferimento agli IP dinamici, che non consentono l'identificazione se non combinando il dato con ulteriori dati in possesso di soggetti terzi, quali i fornitori del servizio di connessione. Con la sentenza citata, resa sulla richiesta di un cittadino tedesco di inibire, in assenza di consenso, la raccolta e conservazione degli indirizzi IP da parte della Repubblica Federale (che agisce come privato in relazione ad alcuni siti relativi a servizi federali), i giudici europei hanno sottolineato che l'indirizzo IP dinamico non può essere considerato in sé stesso un dato personale, in quanto non permette (autonomamente) l'identificazione dell'interessato; tuttavia il medesimo indirizzo IP deve considerarsi dato personale in presenza della possibilità, per il gestore del sito, di "incrociare" il dato con quelli in possesso del fornitore del servizio di connessione, potendo così giungere alla identificazione del visitatore del sito. Sulla sentenza in questione, cfr. F. MERLA, *L'indirizzo IP dinamico quale dato personale,* in *Diritto informazione informatica*, 2017, p. 360 ss.

[33] La tematica dei controlli datoriali sugli strumenti informatici in uso ai lavoratori costituisce oggetto di una copiosa giurisprudenza, nazionale ed internazionale, ultimo esempio della quale può considerarsi la sentenza della Grande Camera della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 nel cd. caso Barbulescu c. Romania, che ha considerato come violazione della riservatezza (art. 8 CEDU) il controllo datoriale sulle email del lavoratore, ribaltando la precedente decisione del 12 gennaio 2016. In precedenza, si erano registrate, in ambito nazionale, situazioni di monitoraggio ed acquisizione dei file di navigazione e dei *cookies*

L'art. 4 n.1) del Regolamento offre una nozione generale, con specificazioni esemplificative e non esaustive (si parla non a caso di "particolare riferimento"): accanto a questa definizione, deve porsi quella dell'art.9 comma I che prevede alcune "categorie particolari di dati personali", per i quali viene posto un generale divieto di trattamento, temperato poi da tutte le ipotesi "eccezionali" (ma si tratta di ben dieci categorie di eccezioni!) poste nel seguito della disposizione[34]. Dispone, in particolare, l' art. 9 comma 1: è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Proprio sull'art.9 possono concentrarsi alcune considerazioni, prendendo le mosse dalla formulazione testuale del comma 1, dalla quale emerge la tecnica normativa utilizzata dal legislatore europeo per evidenziare un rinnovato approccio: il divieto di trattamento di tutti quei dati che, oltre la soglia dei dati comuni, identificano il soggetto nella sua dimensione fisica e altresì in quella sociale contribuendo alla de-costruzione del prisma unitario dell'identità personale, per individuare le molteplici dimensioni della persona[35].

Il comma I, se nella prima parte richiama quanto previsto dall'art.8 della Direttiva 95/46[36], con riferimento ai dati personali che rivelino l'appartenenza razziale o etnica o le

---

nonché di controllo dei flussi di comunicazione sui profili social, che avevano determinato provvedimenti di licenziamento; in giurisprudenza, cfr. Trib. Firenze 02 febbraio 2017, Cass. civ., sez. I, 19 settembre 2016, n.18302, Cass. civ., sez. lav., 27 maggio 2015, n. 10955, Cass. civ., 23 febbraio 2010, n. 4375, Cass. civ. sez. lav., 17 febbraio 2015, n. 3122; in dottrina A. SITZIA, *"Personal computer" e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *ADL*, 2017, p. 804; M. COTTONE, *"Social network": limiti alla libertà di espressione e riflessi sul rapporto di lavoro (il "Like"),* in *Il lavoro nella giurisprudenza*, 2017, p. 382; D. PIZZONIA, A. SITZIA, *Il controllo del datore di lavoro su internet e posta elettronica. Quale riservatezza sul posto di lavoro?,* in *NGCC*, 2016, p. 901 ss.; F. IAQUINTA, A. INGRAO, *La privacy e i dati sensibili del lavoratore legati all'utilizzo dei social networks. Prevenire è meglio che curare,* in *Diritto delle relazioni industriali*, 2014, p. 1027; in margine, sia consentito il riferimento a A. BUSACCA, *I controlli tecno-informatici tra poteri del datore e tutela (dei dati) dei lavoratori*, in *Know.it*, 2017, fasc. 3, 5.

[34] In argomento osserva M. GRANIERI (*Il trattamento di particolari categorie di dati personali nel reg. UE 2016/679,* cit., p. 169) come "l'ampliamento della nozione di dato personale e la sua declinazione come dato che rientra nelle categorie particolari non rappresentano di per sé soli elementi di maggiore tutela, perché paradossalmente la dilatazione di ciò che si intende per dato personale aumenta, anziché diminuire, le difficoltà di effettiva tutela in tutti i contesti di emersione sulle informazioni personali".

[35] A. RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali,* in *Contratto e Impresa*, 2017, p. 586 ss.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo,* in *NLCC*, 2017, p. 410 ss.

[36] L'art. 8 comma 1 della Direttiva 95/46/CE recitava testualmente : "Gli Stati membri vietano il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale"; il d.lgs. 196/2003, sul punto, individua tali dati come "dati sensibili" nell'ambito della definizioni dell'art. 4 (lett. d "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale), rinviando poi al successivo art. 22 per le modalità ed i principi da applicare al trattamento dei dati sensibili. In argomento, nell'ambito della vasta bibliografia, cfr. G. SANTANIELLO (a cura di), *La protezione dei dati personali,* in *Trattato di diritto amministrativo*, Padova, 2005; in particolare, in ordine alla risoluzione di alcune criticità interpretative relative all'ambito di applicazione dell'art. 22 cod. priv., cfr. la recente Cass. ord.

convinzioni religiose e filosofiche, le opinioni politiche o l'appartenenza sindacale, se ne discosta quando contempla "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

L'ambito delle categorie contemplate è davvero molto ampio: basti considerare i dati genetici[37], nonché i dati "dati biometrici"[38]; tali categorie chiamano in causa, quanto a

09.02.2017, n. 3455 (in *NGCC*, 2017, p. 1240, con nota di F. PIRAINO, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità di trattamento*).

[37] L'art. 4 definisce, al punto n.13, i dati genetici come "i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione"; già da una prima lettura della definizione appaiono, in tutta la loro portata, le implicazioni relative alle attività di trattamento di tale categoria di dati che permettono non soltanto di accedere ad informazioni sullo stato di salute attuale della persona, ma altresì di compiere analisi sull'anamnesi (personale e familiare) nonché di effettuare valutazioni con carattere predittivo. Già previsti nell'ambito del d.lgs.196/2003 nell'ambito del titolo V dedicato al trattamento dei dati sanitari, nel capo V rubricato, appunto, "dati genetici", tali dati sono attualmente sottoposti, in Italia, a rigide regole di autorizzazione, posto che, come previsto all'art. 90, "il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità": il argomento, cfr. Cass. 13 settembre 2003, n.21014 (in *Danno e Responsabilità*, 2014, p. 43 ss., con nota di F. AGNINO, *Nozione di dati genetici ed il decalogo di legittimità al loro trattamento*). In argomento, cfr. E. PALMERINI, *Informazione genetica e tutela della persona. Implicazioni giuridiche delle analisi genetiche,* Pisa 2004; W. LATTANZI, *Ricerca genetica e protezione dei dati personali,* in *Trattato di Biodiritto* (diretto da ZATTI, RODOTÀ), *Il governo del corpo*. Milano, 2011, p. 319 ss. (ma spec. 326, *Dati personali, dati genetici e campioni biologici: modelli giuridici di riferimento per la ricerca genetica e nuove tendenze*); R. PACIA, *Ricerca genetica, biobanche e consenso informato,* in *Famiglia e diritto,* 2012, 838 ss.; A. M. CAPITTA, *Conservazione dei "DNA profiles" e tutela europea dei diritti dell'uomo,* in *Archiviopenale.it,* 2013, 34 ss. Con particolare riferimento all'utilizzo dei dati genetici in ambito giudiziario ed all'utilizzo dei dati e profili contenuti nelle biobanche, cfr. L. SCAFFARDI, *Giustizia genetica e tutela della persona*, Padova, 2017.

[38] L'art. 4 definisce, al punto n.14, i dati biometrici come "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"; i sistemi di identificazione biometrici si basano su caratteristiche fisiche (tra le quali, ad es., impronte digitali, altezza, peso, elementi dell'occhio, fisionomia, impronta del palmo della mano e vascolarizzazione) e comportamentali (impronta vocale, firma, movimento di digitazione sulla tastiera) che possono essere univoche (non possedute da due o più individui) o universali, singole o collezionabili (comportamenti ripetuti e misurabili quantitativamente) o permanenti (senza mutazioni dovute al trascorrere del tempo) che vengono acquisite e registrate in un database e permettono l'identificazione (univoca) del soggetto al quale le caratteristiche si riferiscono. Utilizzati inizialmente per finalità di identificazione legata ad esigenze di sicurezza nell'ambito dell'accesso ad aree e locali protetti o per transazioni finanziarie di notevole entità, od ancora finalità di sicurezza pubblica o prevenzione di rischi per la collettività (si pensi all'utilizzo negli aeroporti o alla schedatura di soggetti coinvolti in episodi di criminalità o terrorismo), negli ultimi anni i sistemi di identificazione biometrica (e, quindi, di raccolta dei dati) vengono utilizzati in modo più diffuso e generalista, come sistemi di autenticazione per l'accesso ad ambienti digitali ed a device personali (basti pensare ai sistemi di riconoscimento utilizzati da Samsung ed Apple per gli smartphone dotati di lettore di impronte digitali od al sistema di riconoscimento facciale utilizzato da Apple per l'IPhone X). Proprio in riferimento all'incremento ed alla diffusione di tali sistemi di identificazione, ed alla correlata esigenza di tutela dei dati analizzati e raccolti, si sono registrati alcuni significativi interventi con indicazione delle linee-guida da adottare e con la prescrizione di autorizzazioni e ben precisi limiti per le attività di trattamento, tra i quali devono ricordarsi il "Parere n.3/2012" del Gruppo di lavoro ex art. 29 e, in prospettiva italiana, il

modalità e finalità di trattamento, diverse considerazioni in ordine non soltanto ai soggetti che possono essere a ciò preposti[39], ma anche in ordine alla valutazione preventiva[40] ed ai protocolli di sicurezza che dovranno essere adottati nel trasferimento e nella circolazione dei dati[41].

Se il comma 1 esordisce ponendo il divieto di trattamento con riferimento alle categorie di dati considerati, il comma seguente prevede una serie di eccezioni, che legittimano o rendono lecito il trattamento: nelle lettere da a) a j) vengono infatti individuate una serie di circostanze (sottratte all'applicazione del divieto) che possiamo raccogliere individuando tre macro-categorie, collegate all'interesse per la realizzazione/tutela del quale, le attività di trattamento vengono consentite.

Una prima categoria può individuarsi con riferimento alle ipotesi nelle quali rileva un interesse individuale del soggetto dei cui dati si tratta e cioè che il soggetto abbia dato il suo consenso esplicito per una o più finalità[42] (lett. a), che il soggetto abbia reso manifestamente

---

"Provvedimento generale prescrittivo in tema di biometria" adottato dall'Autorità Garante Privacy nel novembre del 2014 e poi rettificato ed integrato nel gennaio del 2015 (il provvedimento è consultabile al sito www.garanteprivacy.it, con la classificazione doc. web. n. 3701432). In argomento, cfr. P. VALORE, *Rilevamento dei dati biometrici e preventiva notificazione al Garante Privacy*, in *Corriere del Merito*, 2011, p. 1167 ss.; S. GIROTTO, *Trattamento dei dati biometrici e dignità della persona*, in *NGCC*, 2012, 248 ss.; A. SITZIA, *Il trattamento dei dati biometrici dei lavoratori: condizioni d'uso,* in *Il lavoro nella giurisprudenza*, 2012, 391 ss.; M. SALA, *Autenticazione e cifrazione di dati biometrici*, in *Gnosis*, 2016, p. 194 ss.

[39] In particolare, deve considerarsi che, ex art. art.37 comma I lett. c) del Regolamento, nella ipotesi in cui "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10" è obbligatoria la nomina di un *Data Protection Officer*; sulle caratteristiche e sui compiti della figura (nonché per le indicazioni bibliografiche in argomento) si rinvia alla precedente nota n. 24, limitandosi in questa sede ad evidenziare come l'art. 35 comma 5 pone espressamente in capo al DPO l'obbligo di segreto o riservatezza in merito all'adempimento dei propri compiti, con ciò implementando i generali obblighi di riservatezza determinati dalle attività di trattamento dei dati sensibili.

[40] Il trattamento "su larga scala" di categorie particolari di dati ex art.9 comma 1 rientra tra le ipotesi che richiedono, ex art.35 comma 3 lett. b), la cd. "valutazione d'impatto"; si tratta di un documento, redatto dal titolare (con la collaborazione ed assistenza del DPO) nel quale devono essere evidenziati i punti di criticità che possono derivare dalle attività di trattamento dati da eseguire ed altresì devono essere descritte "nel dettaglio, le misure previste per contrastare, coinvolti e della generale conformità della normativa" (in questi termini, G. GIANNONE CODIGLIONE, *Risk-based approach e trattamento dei dati personali*, in S. SICA, V. D'ANTONIO, G. M. RICCIO, *La nuova disciplina europea della privacy,* cit, p. 55 ss (ma spec. p. 68 ss, *Valutazione d'impatto e consultazione preventiva*).

[41] Sul punto, cfr. M. MAGLIO, *Cybersecutity e dati personali*, in M. MAGLIO, M. POLINI, N. TILLI, *Manuale di diritto alla protezione dei dati personali,* cit., p. 719 ss.

[42] Il requisito del consenso informa (e conforma) la principale causa di liceità delle attività di trattamento e, diversamente da quanto previsto nella normativa previgente, non richiede ulteriori requisiti (quali ad es. l'autorizzazione scritta da parte dell'Autorità Garante); l'art.9, sul punto, riprende quanto già previsto dal precedente art. 6 in materia (generale) di consenso al trattamento, ribadendo che esso debba essere esplicito e specifico, cioè rivolto alle finalità individuate e dichiarate dal titolare (una o più finalità specifiche). Il requisito del consenso rappresenta il baricentro della disciplina in materia di liceità del trattamento dei dati personali (in argomento, nell'ambito di una vasta bibliografia, cfr. G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. CUFFARO, V. RICCIUTO, V. ZENO ZENCOVICH, *Trattamento dei dati e tutela della persona,* cit., p. 26 ss; F. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008 (ma spec. 181ss., cap. III, *Regole e limiti del consenso al trattamento: riflessi sulla trasparenza ed equità nei rapporti contrattuali e profili di autonomia*

pubblici quei dati[43] (lett. e) oppure sia in considerazione un interesse vitale dell'interessato o di altra persona fisica e l'interessato sia in stato di incapacità e non possa prestare il proprio consenso[44] (lett.c).

---

assistita,); G. DE MEO, *Autodeterminazione e consenso nella profilazione dei dati personali,* in *Diritto informazione e informatica*, 2013, p. 587 ss.), tuttavia non sono mancati dubbi sulla (attuale) reale portata del consenso, soprattutto in relazione alla sempre maggiore specializzazione tecnologica delle attività di trattamento ed all'utilizzo di modalità automatiche di raccolta dei dati, basati sui file di navigazione o sulla interazione di pagine web : si pensi alle funzioni "like" o "condividi" presenti in siti di informazione, svago o commerciali ma collegate ai principali social network: in argomento od alle clausole di autorizzazione alla condivisione dei contenuti; su questo ultimo profilo, proprio considerando come abitualmente il consenso al trattamento dei dati personali rappresenti la reale controprestazione per l'utilizzo di una serie di servizi (apparentemente) gratuiti, si consideri le recenti istruttorie condotte, in ambito nazionale, dall'Agcm nei confronti di Whatsapp (società di gestione di servizio di messaggistica istantanea e condivisione di contenuti digitali) in relazione alla clausola di utilizzo del servizio che autorizzava la condivisione dei dati da parte di Facebook (società di gestione di servizio di social network che aveva acquisito whatsapp) per finalità pubblicitarie; in argomento, cfr GIANNONE CODIGLIONE, *I dati personali come corrispettivo alla funzione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Diritto dell'informazione e dell'informatica*, 2017, p. 418 ss.

[43] In relazione ai "dati resi manifestamente pubblici dall'interessato", è stato osservato come tale circostanza non si presenti come un elemento di liceità, ma piuttosto come una vera e propria causa di legittimità del trattamento, determinando, quindi, in caso di contestazione, capo all'interessato l'onere di dimostrare la mancanza di "manifesta pubblicità" o l'avvenuta pubblicità senza il consenso o comunque senza/contro la volontà dell'interessato stesso; in tali casi, "la valutazione del titolare con riguardo a questa ipotesi deve avvenire in maniera rigorosa, poiché i casi contemplati dall'art. 9 par. 2, introducono eccezioni al divieto e, come tali, presuppongono un'interpretazione restrittiva, sempre a favore della persona alla quale i dati si riferiscono" (in questo senso M. GRANIERI, *Il trattamento di categorie particolari di dati nel reg. UE 2016/679,* cit., p. 172). Tuttavia a queste considerazioni deve aggiungersi la circostanza della difficoltà di determinazione dell'esatta portata dell'avverbio "manifestamente": proprio in considerazione della moltiplicazione dei flussi di informazione e delle modalità di condivisione dei contenuti, appare opportuno chiedersi quando una condivisione può considerarsi come pubblicità manifesta del dato e quando invece, per i canai utilizzati o per le scelte relative alle privacy policy, si possa parlare, invece, di una limitata circolazione che non coinvolge un "pubblico", ma un numero limitato ed individuabile di soggetti; al riguardo si considerino, come ambienti di circolazione, d esempio, i circuiti whatsapp, la bacheca Facebook (in modalità aperta), la bacheca Facebook (in modalità riservata), la bacheca di un gruppo Facebook chiuso, un blog, un blog ad accesso limitato, una pagina "muro" come bacheca open di un sito di supporter sportivi: già dalla considerazione di questi pochi esempi appare manifesto come uno stesso dato personale (ad esempio un filmato nel quale il soggetto esprime le proprie opinioni e/o preferenze in ordine a convinzioni politiche, sindacali o rappresenta il proprio stato di salute) possa avere una diversa diffusione a seconda del circuito nel quale viene immesso; qualora da tale dato vengo poi diffuso su altro circuito (più ampio) senza il consenso dell'interessato, si sarebbe indubbiamente in presenza di un illecito trattamento di dati e di una situazione di data breach; in argomento, anche con riferimento ad un recente drammatico caso di cronaca, cfr. F. CAMILLETTI, *Alcune considerazioni sui profili giuridici dei "social network"*, in *I Contratti*, 2017, p. 451 ss. (ma spec. p. 461, *La responsabilità dei social network per violazione della privacy*), M. MONTANARI, *La responsabilità delle piattaforme on-line (il caso Rosanna Cantone),* in *Diritto dell'informazione e dell'informatica,* 2017, p. 254 ss.

[44] La finalità di cura in caso di interesse vitale dell'interessato o di altro soggetto (che, ad esempio, condivide con l'interessato il gruppo biologico), rappresenta una condizione di legittimità di utilizzo del dato in considerazione del superiore interesse collegato al bene-vita; in argomento, con riferimento anche alle previsioni del Regolamento, cfr. G. CARRO, S. MASATO, M. PARLA, *La privacy nella sanità*, Milano, 2017; più in generale, sui principi ed i limiti del trattamento dei dati per finalità di cura, cfr. C. FILAURO, *Telemedicina, cartella clinica elettronica e tutela della privacy*, in *Danno e Responsabilità*, 2011, p. 472 ss.; G. GLIATTA, *Il diritto alla*

Una seconda categoria con riferimento all'interesse del titolare del trattamento e dell'interessato, cioè quando il trattamento sia necessario per "assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale"[45] (lett.b); od ancora quando sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, con la duplice condizione 1) che l'ente agisca nell'ambito delle sue legittime attività e 2) con adeguate garanzie e che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità; nonché con l'ulteriore considerazione del divieto di comunicazione all'esterno senza il consenso dell'interessato (lett. d).

Una terza e più ampia categoria può individuarsi con riferimento a tutte le altre ipotesi, che riguardano situazioni di interesse generale, collegate all'attività di giustizia[46] (lett. f.), all'esistenza di un interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, sempre nel rispetto dei principi di finalità e non eccedenza[47] (lett. g), ed alle attività svolte a fini "di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" (lett. j); sempre in questa ampia categoria possono ricondursi le ipotesi previste alle lettere h) ed i), poste a tutela di interessi correlati alla tutela della salute, sia in dimensione individuale che collettiva, anche come prevenzione per il rischio di epidemie o diffusione di nuove patologie trattamento è necessario a fini di archiviazione nel pubblico

privacy in ambito medico: trattamento dei dati sensibili e fascicolo sanitario elettronico, in *Responsabilità civile e previdenza,* 2010, p. 682 ss.; R. TOMMASI, *La difesa della privacy in sanità*, Sant'Arcangelo di Romagna, 2007.

[45] Con riferimento all'ambito dei rapporto di lavoro, al quale è dedicato anche il successivo art. 88 (Trattamento dei dati nell'ambito del rapporto di lavoro), rientrano nella categoria anche i dati raccolti a mezzo strumenti di videosorveglianza e di controllo tecnico-informatico, effettuati per finalità di "controllo difensivo" da parte del datore di lavoro/titolare del trattamento; in argomento, cfr. O. DESSÌ, *Il controllo a distanza sui lavoratori,* Napoli, 2017*;* M. SILVESTRI, *Controlli difensivi del datore di lavoro: limiti alla loro utilizzabilità*, in *Il lavoro nella giurisprudenza*, 2017, p. 865 ss.; G. PROIA, *Trattamento dei dati personali, rapporti di lavoro e l'impatto della nuova disciplina dei controlli a distanza*, in *Rivista italiana di diritto del lavoro*, 2016, 547 ss.; F. SANTONI, *Controlli difensivi e tutela della privacy dei lavoratori* in *Giurisprudenza italiana*, 2016, 145 ss.; V. AMATO, *Legittimità del controllo difensivo occulto attraverso i social network,* in *Il lavoro nella giurisprudenza,* 2015, 989 ss.; M. FERRARO, *Controllo della casella e-mail da parte del datore di lavoro, i c.d. controlli difensivi: una nuova decisione della Suprema Corte*, in *Il diritto del mercato del lavoro*, 2012, p. 372 ss.

[46] A. TORRICE, *La tutela della riservatezza in ambito giudiziario*, in G. SANTANIELLO (a cura di), *La protezione dei dati personali,* cit., p. 461 ss.

[47] Anche in questo caso la formulazione testuale, che riprende una previsione già contenuta nella Direttiva in termini di possibilità rimessa alla determinazione degli Stati membri, presenta alcuni profili di criticità, dal momento che il concetto stesso di "interesse pubblico rilevante" continua ad essere rimesso agli Stati membri, prestando quindi il fianco alla possibilità di diverse interpretazioni (quando non di abusi del concetto) con potenziale frammentazione del quadro di tutela. In particolare, sottolinea M. GRANIERI (*Il trattamento di categorie particolari di dati nel reg. UE 2016/679,* cit., p. 174) in tempi come quelli attuali caratterizzati dall'emersione di "tendenze alla chiusura degli ordinamenti e nuovi tentativi di schedatura" soprattutto in presenza di fenomeni di vasta portata quali i flussi migratori, "al costo di un allungamento della disciplina (…) sarebbe stato meglio specificare quali sono le circostanze nelle quali l'interesse pubblico rilevante permette il trattamento dei dati personali senza il consenso degli interessati, ovvero prevedere che, in casi eccezionali, possa essere la Commissione, su istanza degli Stati membri, ad autorizzare un particolare trattamento o una categoria di trattamenti, anziché lasciare una clausola generale in un contesto di fattispecie puntuali".

interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi[48].

4. *Tra proprietà ed accesso: le "categorie particolari di dati personali" come (necessario) punto di partenza per una rinnovata strategia di* data protection on line

L'analisi, seppure molto veloce, delle ipotesi previste dall'art.9 rende chiaro come, seguendo le parole di uno dei primi commentatori, il legislatore abbia inteso offrire una altalena di regimi, con una diversa considerazione del diritto sui propri dati ora come situazione indisponibile, ora come situazione proprietaria, avvalorando il ruolo del consenso, fino alla considerazione delle ipotesi di circolazione per interesse pubblico superindividuale. Tutto questo, peraltro, come già accennato, "senza decretare la prevalenza dell'uno o dell'altro"[49].

Che il dato personale risponda ad una logica proprietaria non pare possa porsi in discussione, soprattutto laddove esso può validamente costituire oggetto di cessione e circolazione con carattere di esclusiva e vincoli di sfruttamento[50]; maggiori perplessità, su questa qualificazione, possono invece suscitare quelle categorie di dati che non presentano una caratteristica di esclusività, ma di condivisione: il riferimento è indubbiamente ai dati genetici, laddove la compartecipazione del singolo al "gruppo biologico" e, di conseguenza, la possibilità di identificazione non si esaurisce in riferimento all'individuo, ma ad una pluralità di soggetti[51]; in questo senso, la logica proprietaria sembrerebbe dover cedere alla

[48] L'ipotesi prevista alla lettera i, diversamente da quella della lettera c, concerne le ipotesi di trattamento per finalità di interesse pubblico o generale, sopravanzando la dimensione individuale del consenso, proprio nell'ottica di un più ampio ambito di applicazione; in questo senso, cfr. F. MASCHIO, *Il trattamento dei dati sanitari. Regole generali e particolari trattamenti per finalità di rilevante interesse pubblico*, in G. SANTANIELLO (a cura di), *Il trattamento dei dati personali,* cit., p. 485 ss.

[49] Sono parole di M. GRANIERI (*Il trattamento di categorie particolari di dati nel reg. UE 2016/679,* cit., 170) il quale si sofferma sulla diversa considerazione del dato personale e del diritto (dell'interessato) su di esso, "sancendo l'indisponibilità del diritto al primo paragrafo, degradandolo a diritto di natura proprietaria nel secondo – soprattutto nella lettera a, dove si espande significativamente il ruolo del consenso – e poi avallando tutta una serie di deroghe nelle quali la base giuridica del trattamento prescinde dal consenso, con una tendenza che sembra deporre per una diffusa *liability rule*, dove tuttavia l'accesso al dato non avviene in cambio di un corrispettivo, ma per l'esercizio di funzioni che talora hanno a riguardo l'interesse dell'individuo ed altre volte concernono l'interesse generale dello Stato, ovvero l'esercizio di libertà fondamentali di terzi".

[50] F. VITERBO, *Protezione dei dati e autonomia negoziale, cit.*, p. 121 ss; G. RESTA, *Contratto e diritti della personalità*, in V. ROPPO (a cura di), *Trattato del Contratto. VI. Interferenze*, Milano 2006, p. 3 ss. (ma spec. p. 59 ss., *La circolazione dei diritti sugli attributi immateriali*).

[51] Sul portato del ricorso, sempre più generalizzato alle prove biologiche, sia in ambito civilistico che penalistico, si è affermata una nuova concezione del gruppo familiare, individuando la cd. "famiglia biologica" come formazione sociale "distinta dalla comunità familiare fino ad oggi presa in considerazione dal diritto" e che comprende individui accomunati dalla condivisione dei dati genetici; proprio con riferimento alla "famiglia biologica" considerata in tutte le sue componenti, "la riferibilità soggettiva del dato ad un gruppo,

diversa considerazione dell'accesso[52] o, in ogni caso, ad una condivisione non esclusiva, che tuttavia, potrebbe porre in dubbio la validità del consenso individuale, a meno di non offrire una diversa e più restrittiva considerazione del principio di finalità o del più generale principio di minimizzazione di trattamento del dato.

Per le categorie ex art.9, lasciando da parte l'ipotesi della lett. a), cioè il consenso dell'interessato, in tutte le altre ipotesi possono individuarsi condizioni di circolazione e liceità delle attività di trattamento che non integrano scambi o prestazioni corrispettive, ma sono rivolte al soddisfacimento di interessi dell'interessato, del titolare o della collettività.

Se invece andiamo a considerate proprio la circolazione che avviene con il consenso dell'interessato, cioè le ipotesi sub lett. a), appare necessario porre attenzione al contemperamento della disposizione con le ipotesi di trattamento effettuato nelle aree "di mercato", cioè in tutte quelle ipotesi nelle quali la circuitazione delle informazioni costituisca corrispettivo di un servizio[53] e venga integrata in attività di monitoraggio o profilazione: si pensi non soltanto alla navigazione nei siti e.commerce, ma anche alla raccolta dati effettuata tramite social network per finalità non di carattere personali (e quindi escluse dalla *household exception* del considerando 18[54]), od ancora alla raccolta dati

---

anziché al singolo, prospetta l'eventualità di conflitti interindividuali per l'accesso all'informazione ed il successivo controllo: ad esempio l'interesse ad acquisire caratteristiche geniche e l'interesse a non sapere; tra l'interesse a mantenere la riservatezza sulle informazioni raccolte ed esigenze, di vario genere, la cui soddisfazione presuppone, invece, di accedervi" (le espressioni sono di E. PALMERINI, *Informazione genetica e tutela della persona,* cit., p. 34 ss.

[52] Il passaggio "dalla proprietà all'accesso", individuando quest'ultimo come "metafora più efficace della una nuova era" e "potente strumento concettuale per riformulare una visione del mondo e dell'economia" è stato teorizzato, già all'alba del nuovo millennio da Jeremy RIFKIN; lo stesso titolo della famosa opera, indicata nella traduzione italiana, come "*l'era dell'accesso*" (Milano, 2000) passò poi, in chiave più generalizzata, ad indicare l'età attuale, segnata dalla dematerializzazione e dal passaggio da una logica proprietaria basata sul binomio proprietà/possesso ad una diversa impostazione basata sul binomio accesso/utilizzo; ma ben più significativo è, invece, il titolo originale completo *The Age of Access: The New Culture of hypercapitalism, where all of life is a paid-for Experience* (edito da Tarcher/Penguin, New York), che evidenzia già la matrice economica dell'analisi della nuova cultura basata non più sulla apprensione materiale e sulla proprietà intesa come titolarità e rapporto col bene, ma piuttosto sulla condivisione esperienziale e sull'utilizzo di un servizio o di una utilità che non si proiettano in realtà materiale, ma ineriscono/connotano/migliorano la qualità della vita della persona.

[53] G. GIANNONE CODIGLIONE, *I dati personali come corrispettivo alla funzione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in *Diritto dell'informazione e dell'informatica*, 2017, p. 418 ss.

[54] Il Considerando n. 18 pone una limitazione di operatività per le norme del Regolamento, individuando alcuni trattamenti che ne restano esclusi in ragione nella natura e delle finalità spiccatamente private (Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico); appare subito chiaro come il riferimento alla circolazione dei dati attraverso i social possa costituire una zona d'ombra, soprattutto per tutte quelle situazioni ibride o di collegamento automatico, che potrebbero, quindi, sottendere delle attività di trattamento e raccolta dati in assenza di consenso (anche solo di consapevolezza sulla raccolta stessa) da parte dell'interessato.

effettuata tramite *cookies*[55]; in ognuna di queste ipotesi il consenso del soggetto, esplicito ma più o meno consapevole (soprattutto per i *cookies*, il click sul tasto accetto costituisce una rapida modalità per proseguire la navigazione, spesso incuranti del valore dei dati che si mettono in circolo), può determinare una attività di trattamento per una categoria di dati che rientra tra quelle dell'art.9 comma 1; a titolo esemplificativo si considerino la visita (e relativo cookie) ad una videoteca oppure ad un portale con filmati che possano permettere di ricostruire l'identità o le preferenze sessuali; la registrazione sul form di un sito e-healt (ed al riguardo basta consultare il report E.commerce Italia 2017 per verificare l'incremento delle transazioni commerciali on line di farmaci e di dispositivi paramedicali[56]); il click sul "like" o la condivisione di pagine Facebook[57].

La semplice individuazione delle categorie, allora, non può che costituire il punto di partenza per la determinazione di modalità sicure di circuitazione dei dati e strumenti di

[55] Rinviando alla precedente nota 24 per quanto riguarda la considerazione dei cookies nell'ambito dei *recognition identifiers*, con riferimento alla attuale regolamentazione delle attività di raccolta dati attraverso i cookies, cfr. C. ROSSI CHAUVENET, E. STEFANINI, *Internet e privacy. Il recepimento in Italia della Direttiva sulla "cookie law",* in *Responsabilità civile e previdenza*, 2012, p. 1806 ss; A. MANTELERO, *Si rafforza la tutela dei dati personali: data breach notification e limiti alla profilazione mediante i cookies*, in *Diritto dell'informazione e dell'informatica*, 2012, 781 ss.; M. VIGGIANO, *"Navigazione" in Internet ed acquisizione occulta di dati personali, ivi*, 2007, 347 ss; V. CARIDI, *La tutela dei dati personali in Internet: la questione dei logs e dei cookies alla luce delle dinamiche economiche dei dati personali,* in *Diritto dell'informazione e dell'informatica,* 2001, p. 763 ss.

[56] *E-commerce in Italia: ritardi e potenzialità.* rapporto sull'e-commerce: Report a cura della BEM rese@arch (on line sub https://www.bemresearch.it/report/ecommerce-italia), *E.Commerce in Italia 2017*, Report a cura della Casaleggio Associati (www.casaleggio.it/pubblicazioni/focus/e-commerce-in-italia-2017.php) basato su dati raccolti attraverso intervista e questionari compilati da circa 340 aziende e contatti con circa 3000 aziende; Rapporto 2016 dell'Osservatorio eCommerce B2C della School of Managment del Politecnico di Milano (http://www.osservatori.net/ecommerce_b2c).

[57] Sui potenziali "rischi" derivanti dalla circolazione dei dati e delle informazioni tramite social network, deve evidenziarsi, tuttavia, che l'utilizzo stesso del social una percentuale di rischio che l'utente sceglie di accollarsi con la stessa adesione, cioè con l'accettazione delle clausole contrattuali e delle *privacy policies*; nel sottoscrivere l'adesione (cioè nel concludere il contratto per l'utilizzazione del social network in questione) deve considerarsi che, proprio in considerazione delle modalità tecniche di funzionamento e di interconnessione delle pagine web, non è remota l'eventualità che altri possano individuare e riconoscere le tracce e le informazioni lasciate in un determinato momento sul sito, anche a prescindere dal consenso: si pensi, ad esempio, dell'attività di c.d. "*tagging*" (tradotta in lingua italiana con l'uso del neologismo *"taggare"*) che consente, ad esempio, di copiare messaggi e foto pubblicati in bacheca e nel profilo altrui oppure email e conversazioni in *chat*, che di fatto sottrae questo materiale dalla disponibilità dell'autore e sopravvive alla stessa sua eventuale cancellazione dal social network. Proprio negli ultimi anni, peraltro, si sono intensificati gli studi rivolti alla tutela dei dati in relazione alla circolazione tramite social: in argomento, cfr. F. CAMILLETTI, *Alcune considerazioni sui profili giuridici dei social network,* cit., 461; E. FALLETTI, *I "social network": primi orientamenti giurisprudenziali*, in *Corriere giuridico*, 2015, p. 992 ss.; F. ZANI, *Il difficile bilanciamento fra tutela della libertà di manifestazione del pensiero e diritto alla riservatezza nell'era dei social network*, in *Osservatorio costituzionale*, 2/2014; C. PERLINGIERI, *Profili civilistici dei social network*, Napoli, 2014; F. AGNINO, *Fino a che punto è possibile disporre contrattualmente dei propri diritti? (vedi contratto FB)*, in *Giur. merito*, 2012, p. 2555 ss.; P. GALDIERI, Il *trattamento illecito del dato nei social network*, in *Giur. merito*, 2012, p. 2697 ss.; L. PICOTTI, *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giur. merito*, 2012, p. 2522 ss.; A. OTTOLIA, *Privacy e social networks: profili evolutivi della tutela dei dati personali*, in *AIDA*, 2011, p. 360; R. CATERINA, *Cyberspazio, social network e teoria generale del contratto*, in *AIDA*, 2011, p. 93 ss.; in margine sia consentito il rinvio a A. BUSACCA, *Circolazione delle informazioni sui social network e tutela della identità digitale*, in P. CENDON (a cura di), *Trattato dei nuovi danni*, vol. III, Padova, 2015, p. 259 ss.

tutela in grado di ridurre al minimo i rischi dei cd. *data breach*, proprio in forza dell'approccio precauzionale del quale si è detto.

Sebbene appaia comunque chiaro che la considerazione delle categorie particolari dei dati costituisce, nell'ottica del legislatore europeo, l'implemento qualitativo della tutela, ad essa deve affiancarsi il valore fondamentale della valutazione d'impatto preventiva e della scelta di adeguate policy di *risk management:* una valutazione puntuale e relata alla tipologia ed alla qualità/quantità dei dati oggetto del trattamento ed una previsione dell'utilizzo delle nuove tecnologie e delle nuove circuitazioni dei flussi informativi e documentali pongono alle legislazioni nazionali la sfida per la realizzazione di uno standard di tutela uniforme, in grado di proiettarsi verso la dimensione di quello che è stato già definito come l'imminente avvento del web 3.0[58].

[58] "Con il web 3.0 si apre un panorama ancora più complesso in cui entrano in gioco direttamente gli oggetti e gli strumenti tecnici attraverso i quali le informazioni ed i dati vengono raccolti. Questi apparati infatti non sono solo capaci di accumulare un considerevole flusso di informazioni riguardanti coloro che li utilizzano, ma riescono addirittura ad entrare in collegamento in modo del tutto autonomo, con altri dispositivi ed interagire fra di loro per cambiarsi ed aggiornare tutte le informazioni in loro possesso": in questi termini, G. MARINI, *Diritto alla Privacy, in Commentario al Codice Civile* (a cura di GABRIELLI*), Delle Persone.* Vol. III. *Leggi collegate* (a cura di V. BARBA, S. PAGLIANTINI), Milano, 2013, p. 199 (ma spec. p. 252 ss., *Web 3.0. La Nuvola e le altre frontiere tecnologiche*).