JUS CIVILE

CLAUDIA IRTI

Professore associato di diritto privato – Università Ca' Foscari di Venezia

DATO PERSONALE, DATO ANONIMO E CRISI DEL MODELLO NORMATIVO DELL'IDENTITÀ

1. – Il Codice in materia di protezione dei dati personali, così come modificato dal d.lgs.10 agosto 2018, n. 101, in adeguamento al regolamento UE 2016/679/UE (GDPR), non contiene più alcun riferimento alla locuzione "identità personale" [1], come si premurava di fare, invece, l'art. 1 dell'originario testo normativo [2], prima delle intervenute modifiche [3].

---

[1] Una "locuzione" cui nel tempo sono stati ascritti vari significati, in relazione ai contesti e in ragione delle funzioni che le sono state attribuite, e che ancor oggi, nonostante i risultati raggiunti, resta soggetta ad un continuo processo di trasformazione: P. GLEASON, *Identifying Identity: A Semantic History*, *Journal of American History*, LXIX, 1983, p. 4 ss.; il problema della definizione giuridica del diritto all'identità è affrontato da L. TRUCCO, *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*, Torino, 1976, p. 223.

[2] Art. 1, legge 31 dicembre 1996, n. 675: "La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all´identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione" – è poi trasmigrato nell'art. 2 del Codice in materia di protezione dei dati personali (d.lgs. n. 196 del 2003) che, prima della recente rivisitazione recitava "Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

[3] La citata norma, pur contemplando la nozione d'identità personale, non ne forniva, tuttavia, una definizione. Secondo alcuni, il legislatore avrebbe fatto un rinvio implicito alle definizioni già elaborate in giurisprudenza e in dottrina, così G. PINO, *L'identità personale*, in *Trattato di biodiritto*, diretto da S. RODOTÀ e P. ZATTI, in *Ambito e fonti del diritto*, a cura di S. RODOTÀ e M. TALLACCHINI, Milano, 2010, p. 297 ss., p. 304.

La novità non può passare inosservata.

Il diritto all'identità personale [4] ha rappresentato, nel nostro ordinamento, il perno attorno al quale – a partire dalla metà degli anni Settanta del secolo scorso, grazie agli sforzi interpretativi di dottrina e giurisprudenza – la tutela dell'individuo, nella sua unitarietà e unicità, si è sviluppata.

Un diritto, si sottolinea [5], sconosciuto ad altre esperienze giuridiche, che tuttavia non può non essere percepito come un traguardo fondamentale nella strada che conduce alla piena valorizzazione dell'individuo, di "quell'unico e unitario bene che è (…) la stessa persona umana" [6].

Per lungo tempo la dottrina si è posta il problema della ricerca di un "fondamento positivo" [7] del diritto all'identità personale, ragione per cui non sorprende che la citata norma fu salutata come il simbolico "approdo normativo" di quel processo giurisprudenziale e dottrinale che aveva condotto alla ricostruzione giuridica della stessa nozione di "identità personale", nonché il momento a partire dal quale la "categoria" può considerarsi definitivamente ricondotta nel quadro dei diritti e delle libertà fondamentali [8].

---

[4] A. DE CUPIS, *Il diritto all'identità personale*, Milano, 1949; G.B. FERRI, *Privacy e identità personale*, in *Riv. dir. com*., 1981, II, p. 379 ss.; F. MACIOCE, *Tutela civile della persona e identità personale*, Padova, 1984; V. ZENO-ZENCOVICH, voce *Identità personale*, *Dig. disc. priv.*, Sez. civ., IX, p. 294 ss.; L. VALLE, *Il diritto all'identità personale*, in M. SESTA e V. CUFFARO (a cura di), *Persona, famiglia e successioni nella giurisprudenza costituzionale*, Napoli, 2006, p. 77 ss.; P. ZATTI, *Dimensioni ed aspetti della identità nel diritto privato attuale*, in *L'identità nell'orizzonte del diritto privato*, *supplemento a Nuov. giur. civ. comm*., 4, 2007, p. 1 ss.; G. FINOCCHIARO, voce *Identità personale (diritto alla*), in *Dig. disc. Priv.* sez. civ., Aggiornamento, Torino, 2010; AA.VV., *Il diritto alla identità personale*, a cura di G. ALPA E M. BESSONE, Padova, 1981; AA.VV., *La lesione dell'identità personale e il danno non patrimoniale*, *Atti del seminario promosso dal centro di iniziativa giuridica P. Calamandrei a Messina il 16 aprile 1982*, Milano, 1985.

[5] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da G. FINOCCHIARO, Bologna, 2017, p. 3.

[6] P. RESCIGNO, voce *Personalità (diritti della)*, in *Enc. gir. Treccani*, vol. XXVI, p. 1 ss., a p. 2.

[7] Al riguardo G. RESTA, *I diritti della personalità*, in *Le persone fisiche e i diritti della personalità*, a cura di G. ALPA e G. RESTA, *Trattato di diritto civile*, a cura di R. Sacco, 2006, p. 361 ss. a p. 543, ove si osserva come in assenza di specifiche disposizioni codicistiche il fondamento positivo della tutela viene identificato direttamente nell'art. 2 della Costituzione; cfr. in argomento P. ZATTI, *Il diritto all'identità e l'"applicazione diretta" dell'art. 2 Cost*., in AA.VV., *Il diritto alla identità personale*, a cura di G. ALPA e M. BESSONE, Padova, 1981, p. 55 ss. per un'attenta discussione sulle premesse e sulle implicazioni di una siffatta tecnica argomentativa. L'utilizzo dell'art. 2 della Costituzione come "clausola aperta e generale di tutela del libero e integrale svolgimento della persona umana" che come tale può abbracciare il diritto all'identità personale quale diritto che "mira a garantire la fedele e completa rappresentazione della personalità individuale del soggetto" (Corte di Cassazione, 22 giugno 1985, n. 3769) è, peraltro, contrastata dai sostenitori di una lettura "restrittiva" della norma, per tutti A. PACE, *Il c.d. diritto all'identità personale e gli art. 2 e 21 della Costituzione*, in *Il diritto all'identità personal*e, cit., *passim*.

[8] S. RODOTÀ, *Tecnopolitica*, 2004, Roma-Bari, p. 134 ss.

Ebbene, in virtù della ricezione del nuovo testo normativo [9], cade il riferimento al concetto di "identità personale", come cade, del resto, il riferimento alla dignità [10], elementi, entrambi, che Stefano Rodotà [11], all'indomani della promulgazione del (primo) Codice della Privacy, aveva segnalato come significative "valorizzazioni della norma italiana rispetto allo schema di riferimento della Direttiva", un "arricchirsi del quadro dei principi" che conferma "la dilatazione della considerazione normativa" [12].

L'orizzonte di tutela, nel suo enunciato letterale, torna a far riferimento ai soli "dati personali riferibili alle persone fisiche", a quei "frammenti" in cui d'identità, disgregatasi nell'impatto con il mondo virtuale, si disperde e si moltiplica.

---

[9] Il regolamento, come noto, è strumento di armonizzazione massima che non ammette – diversamente da quanto è accaduto con il recepimento della direttiva 95/46/CE – margine di manovra al legislatore nazionale.

[10] Il collegamento fra privacy e dignità è dovuto, soprattutto, all'elaborazione della giurisprudenza tedesca. Come noto la Carta Fondamentale tedesca contiene un espresso riferimento alla "protezione della dignità umana" come diritto fondamentale, cui è dedicato – significativamente – il primo articolo della Carta. Questa norma, posta in relazione con il comma 1, art. 2 della stessa Carta, a norma del quale "ognuno ha diritto al libero sviluppo della propria personalità, in quanto non violi i diritti degli altri e non trasgredisca l'ordinamento costituzionale o la legge morale" ha reso possibile sviluppare l'idea che la "privacy" dei dati personali sia considerata parte integrante della dignità della persona. Sul collegamento fra privacy e dignità si veda S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa. Il nuovo codice della privacy*, in *Eur. e dir. priv*., 2004, 1, p. 1 ss.; più in generale sulla dignità come valore supremo e unificante, onnicomprensivo degli aspetti fondamentali (genetico, corporale e psicologico formale) che formano il nucleo dell'identità si veda P. ZATTI, *Maschere del diritto volti della vita*, Giuffrè, 2009, p. 37 ss.

[11] *Persona, riservatezza, identità, Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. Dir. priv.*, 1996, p. 583 ss.

[12] Una lettura critica della precedente impostazione legislativa "basata sulla prevalenza del principio personalistico e, in particolare del principio della dignità umana", è data da F. BRAVO, "*Il "diritto" a trattare dati personali nello svolgimento dell'attività economica"*, Milano-Padova, 2018, p. 195 ss. il quale sottolinea come "l'evoluzione sociale, economica istituzionale e tecnologica porta il legislatore eurounitario a considerare nuove istanze, di fronte alle quali l'autodeterminazione informativa e il principio di dignità – realizzati con i meccanismi di protezione dei dati personali – vengono mitigati di fronte ad altre istanze, volte a favorire la libertà di circolazione dei dati e l'integrazione del mercato, che ora procede di pari passo con quella politica, istituzionale e sociale".

Critica, anche, la posizione di V. RICCUTO, *La patrimonializzazione dei dati personali, contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, p. 689 ss.; ID., *La patrimonializzazione dei dati personali*, in AA.VV., *I dati personali nel diritto europeo*, a cura di V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, p. 27 ss., ove l'autore sostiene che la prima disciplina di matrice comunitaria relativa alla privacy, la direttiva 95/46, avrebbe potuto essere letta in una prospettiva "patrimonialistica" (sollevata da qualche pioneristico commentatore quale S. SIMITIS, *Il contesto giuridico e politico della tutela della privacy*, in *Riv. crit. dir. priv*., 4, 1997, p. 575 ss.) che, tuttavia, "la normativa italiana di recepimento disattenderà … rimanendo, in buona sostanza, ancorata ad una (sola) lettura assolutistica della persona"; C. CAMARDI, *Mercato delle informazioni e privacy. Riflessioni generali sulla L. n.665/1996*, in *Eur. dir. priv*., 1998, p. 106 ss., *passim*.

La norma, è stato rilevato, si limita a proteggere il frammento ma non l'insieme [13].

Questa, invero, la conseguenza giuridica di una realtà fenomenologica che, già da tempo – nel passaggio dall'identità personale all'identità digitale [14] – ha visto l'unità identitaria del singolo scomporsi in "un sistema informazionale complesso" costituito da una somma di dati che ne rappresentano e costituiscono l'essenza, ma che allo stesso tempo sono soggetti a manipolazioni e ricomposizioni fittizie [15]. L'ineludibilità dell'elemento fenomenologico ha spostato al centro del sistema politico-istituzionale l'attenzione sul dato personale, il quale, tuttavia, non è tutelato "in sé e per sé" ma continua a esserlo in via mediata, in quanto rappresentazione della persona da cui promana [16], veste in virtù della quale la protezione dei dati personali assurge – a sua volta – all'olimpo dei diritti fondamentali dell'individuo.

2. – Fin dal tempo della direttiva madre [17] il legislatore europeo ha concentrato la sua attenzione sulla tutela del "dato personale", qualificando come tale "qualsiasi informazione concernente una persona fisica identificata o identificabile ('persona interessata')".

Tale nozione determina l'ambito di applicazione materiale della normativa sulla protezione dei dati, in quanto, solo in caso di trattamento di "dati personali", si applicano i principi, i diritti e gli obblighi ivi previsti (articolo 3, paragrafo 1, della vecchia DPD e articolo 2, paragrafo 1, del GDPR) [18].

Riuscire a definire con esattezza cosa s'intenda con questa locuzione [19] è, di conse-

---

[13] Così sintetizza efficacemente G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, cit.

[14] G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, 3, p. 516.

[15] G. MARINI, *La giuridificazione della persona idee e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, p. 359 ss., a p. 387.

[16] G. ALPA, *La proprietà dei dati personali*, in *Persona e mercato dei dati. Riflessione su GDPR*, a cura di N. Z. GALGANO, Milano-Padova, 2019, p. 9 ss.

[17] L'art. 2, comma 1, lett. a) della direttiva 95/46/CE, definiva i "dati personali" come: "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".

[18] Non deve pertanto stupire che il recente GDPR, nel mantenere come obiettivo "la tutela dei diritti e le libertà fondamentali delle persone fisiche", sia andato a sostituire il riferimento specifico al "diritto fondamentale alla vita privata" con quello relativo alla "protezione dei dati personali" (articolo 1, paragrafo 2 del GDPR).

[19] La nozione di dato personale è stata approfonditamente indagata in un corposo studio – "*What are personal data?*" – che la UK Information Commission ha nel 2004 commissionato all'Università di Shef-

guenza, presupposto essenziale per comprendere quale sia l'ambito effettivo di estensione della tutela ad essi riconosciuta.

Partendo dalla definizione giuridica si può certamente affermare che i "dati personali" sono "informazioni"; una locuzione che, tuttavia, si presta a plurime interpretazioni, un termine dal significato ambiguo, multiforme, comunemente utilizzato – per esempio – tanto per far riferimento all'informazione come "contenuto", quanto al supporto materiale che immagazzina quel contenuto.

Per meglio comprendere quale sia il significato d'informazione richiamato dalla disciplina normativa in materia di privacy può tornare utile la classificazione elaborata da un autore, Herbert Zech [20], il quale propone di distinguere tra informazioni semantiche [21],

---

field al fine di favorire la comprensione della locuzione "dati personali" e contribuire a darne una definizione coerente e attendibile. La ricerca è stata condotta utilizzando più chiavi di lettura – giuridica, sociologica e psicologica – nonché attraverso un'indagine empirica su come il termine "dati personali" sia stato interpretato e applicato dalle autorità preposte alla protezione dei dati nelle diverse giurisdizioni europee. Il risultato più interessante raggiunto da questo studio è stata la identificazioni di diversi "modelli teorici" (Ideal Types) di classificazione dei dati personali, mediante l'utilizzo del criterio centrale di rilevanza/irrilevanza del "contesto": i Paesi che adottano il criterio della "irrilevanza del contesto" suggeriscono, esplicitamente o implicitamente, che può essere redatto un elenco di dati che sono sempre (e/o mai) dati personali; il contesto non è considerato un fattore cruciale per determinare se i dati debbano essere classificati come "personali". I Paesi che, invece, adottano il criterio della "rilevanza del contesto" classificano (quasi) tutti i dati come "talvolta" in grado di essere qualificati come dati personali, nel senso che tutti i dati potrebbero essere qualificati come dati personali "nelle giuste circostanze". Di conseguenza, questi Paesi ritengono che non sia possibile stilare un elenco definitivo di dati che costituiranno sempre (o mai) 'dati personali'. Lo studio, analizzate le differenze, propone diversi "modelli teorici" di classificazione: a) il modello "identificatore unico", per il quale i dati personali sono dati che possono essere collegati in modo univoco ad un individuo e rispetto ai quali il contesto è irrilevante; b) il modello "identificatore dipendente dal contesto", secondo il quale i "dati" sono considerati "personali" se possono essere utilizzati per identificare un individuo, in quanto qualsiasi informazione può essere utilizzata, in circostanze appropriate, per identificare una persona; c) il modello che si basa sulla "possibilità (probabilità) di un effetto rilevante" che si fonda su un concetto che definisce i dati quali "personali" solo se in grado di "incidere" materialmente su una "persona identificabile" mala capacità dei dati di incidere sulla privacy di una persona può essere valutata in modo indipendente dal contesto; d) Il modello che si basa sulla "possibilità/probabilità dell'effetto rilevante dipendente dal contesto", in ragione del quale i "dati personali" sono dati in grado di incidere sulla "privacy" di un individuo e il fatto che una particolare informazione sia in grado di incidere sulla vita privata di un individuo è determinato dalle circostanze contingenti del caso specifico ovvero dal contesto. Lo studio è reperibile sul sito https://www.frareg.com/cms/wp-content/uploads/personal_data.pdf.

[20] H ZECH, *Information us a property*, *6 JIPITEC 192*, para 1, 2015; ID., *A legal framework for a data economy in the European Digital Single Market: rights to use data, Journal of Intellectual Property Law & Practice*, vol. 11, n. 6, 2016, p. 460 ss.; ID. *Data as a Tradeable Commodity*, in AA. VV., *European Contract Law and the Digital Single Market*, edited by A. DE FRANCESCHI, Cambridge, Intersentia, 2016, p. 51 ss.

[21] A ben guardare di "ambito semantico del termine informazione" che legittima "l'unificazione di informazioni (nel senso di notizie) … e 'beni informazionali' (nel senso tanto di informazioni 'trattate' che di procedure tecniche del loro trattamento), che l'osservazione della realtà propone al giurista" già aveva parla

ovvero informazioni con un certo significato, informazioni sintattiche, ossia informazioni rappresentate da una certa quantità di segni, e informazioni strutturali, rappresentate dalla struttura di un oggetto fisico. "Ognuno dei tre tipi di informazioni" aggiunge l'autore "può essere trovato nella vita quotidiana: quando parliamo di una notizia, di una storia o del "contenuto" di un libro ci riferiamo al livello semantico. La composizione di un testo o di un file si riferisce al livello sintattico. Infine, quando abbiamo a che fare con un CD, o un libro stampato, ecc. ci riferiamo al livello strutturale. Naturalmente i tre livelli sono collegati, in quanto il significato può essere contenuto all'interno di un testo e un testo può essere stampato. Così, lo strato fisico porta lo strato sintattico e lo strato sintattico lo strato semantico. Tuttavia, da un punto di vista economico e giuridico, ogni livello rappresenta una possibilità indipendente di definire una certa quantità d'informazioni … In economia l'informazione è molto spesso utilizzata nel senso d'informazione semantica. Sapere qualcosa significa avere accesso alle informazioni semantiche. Di conseguenza, un'invenzione (intesa come conoscenza applicata) è un'informazione semantica. Altri esempi d'informazione semantica sono le notizie, i dati personali, i segreti commerciali, etc. …".

Una prima definizione di dati (personali) può essere, dunque, data da un punto di vista semantico, considerando come tali quelle informazioni che hanno "un certo significato", informazioni che descrivono qualcosa (riferibile ad una persona fisica) cui sia possibile dare un senso [22] (a prescindere dallo strumento sintattico e dal supporto materiale utilizzato per "esprimere" e "contenere" l'informazione).

Altri studiosi [23], tuttavia, inducono a riflettere su come, sebbene l'uomo abbia da sempre attribuito "un senso" alle informazioni utilizzando strumenti di misurazione e analisi quali il linguaggio e la matematica, l'arrivo e la proliferazione delle nuove tecnologie abbia accelerato questo processo, consentendo la misurazione, l'analisi e quindi l'utilizzo di dati molto eterogenei, anche dati apparentemente "insignificanti". Ciò comporta che le stesse informazioni, gli stessi dati, possano avere nessun significato o significati diversi a seconda di chi li

---

D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 339 ss. a p. 340, il quale rinvia a P. CATALÀ, *Ebauche d'une théorie juridique de l'information*, in *Inf. e dir.*, 1983, p. 1 ss.

[22] "Data is a description of something that allows it to be recorded, analyzed, and reorganized", così L. FLORIDI, '*Philosophical Conceptions of Information'*, in G. SOMMARUGa (edited by), *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information*, Springer, 2009, p. 13 ss.

[23] N. PURTOVA, *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 2018, p. 40 ss.

percepisce [24]: mentre la mente umana è limitata e non è sempre in grado di ricondurre i dati a "un significato", il modo in cui tutti i nuovi processori attribuiscono significato ai dati è molto diverso e molto più veloce. Il senso della parola "significato" rispetto alle capacità di comprensione dei dati da parte dei moderni computer è fuori dalla portata di qualsivoglia mente umana e molti dati colloquialmente denominati "raw" (grezzi), che non hanno alcun significato o hanno un significato molto limitato per la mente umana, possono acquisire "significato" una volta sottoposti al trattamento degli elaboratori [25].

Procedendo nell'analisi della nozione di dato personale [26] – intesa come "qualsiasi informazione riguardante una persona fisica identificata o identificabile" – indispensabile è soffermarsi sul concetto di "identificabilità" della persona [27], che ha per lungo tempo rappresentato il primo discrimine per garantire la tutela del dato personale. A norma dell'art. 4 (1) del GDPR "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

---

[24] M. BURGIN, *Theory of Information. Fundamentality, Diversity and Unification*, World Scientific Publishing, 2010, p. 6.

[25] Non sorprende, dunque, che The Article 29 Working Party, nel parere non vincolante 4/2007 sul concetto di dati personali, reperibile on line (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_it.pdf), dopo aver suddiviso la definizione di dati personali in quattro elementi – (a) informazioni, (b) relative a (c) una persona fisica (d) identificata o identificabile – analizzando la nozione di "informazione" abbia sostenuto che qualsiasi informazione possa rientrare nel concetto di "dati personali" indipendentemente dalla sua natura, contenuto o formato (veritiera o inesatta, oggettiva e soggettiva, comprese le opinioni e le valutazioni). L'informazione non deve necessariamente riguardare la vita privata o familiare e potrebbe riguardare anche altri aspetti della vita dell'individuo, relativi ad esempio alle sue capacità professionali e di altro tipo. Infine, le informazioni possono costituire dati personali, indipendentemente dal formato, dal supporto o dalla forma, ossia possono essere "alfabetici, numerici, grafici, fotografici o acustici", "conservati su carta [o] in una memoria di computer" come codice binario, strutturati o non strutturati, purché siano soddisfatti gli altri criteri della definizione.

[26] All'interno della categoria "dati personali" sono ricomprese una serie di "sottocategorie" qualificate all'art. 9 del GDPR quali "categorie particolari" di dati personali – tra le quali si distinguono, in quanto rese oggetto di specifica definizione, i "dati genetici", i "dati biometrici" e i "dati relativi alla salute" – che sono assoggettati ad un trattamento di tutela più stringente.

[27] Le maggioranza degli studiosi si sono concentrati su questo elemento del concetto di dati personali fatta propria dagli atti normativi; oltre a quelli già citati, P. OHM, *Broken promises of privacy: Responding to the surprising failure of anonymization*, in *UCLA L. Rev*., 57, 2010, 1701.; L. SWEENEY, '*Simple Demographics Often Identify People Uniquely*', Carnegie Mellon University, Data Privacy Working Paper, 2000, *http://dataprivacylab.org/projects/identifiability/paper1.pdf*.; P SCHWARTZ, D. SOLOVE, '*The PII Problem: Privacy and a New Concept of Personally Identifiable Information'* 86 *N.Y.U. L. Rev.* 1814, 2011, p. 1877. Nel panorama italiano, R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0, una lettura civilistica comparata*, in *Le definizioni nel diritto*, Atti delle giornate di studio 30-31 ottobre 2015 Università di Trento, a cura di F. CORTESE, M. TOMASI, 2016, p. 143 ss.; G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e big data*, in AA.VV., *La privacy digitale*, a cura di E. TOSI, Torino, 2019, p. 447 ss., spec. p. 472 ss.

online o a uno o più elementi della sua identità fisica, fisiologica, genetica, psichica, economica, culturale e sociale"; a ciò si aggiunga che secondo le indicazioni del considerando 26 del GDPR "… per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica, direttamente o indirettamente" e "per accertare la 'ragionevole probabilità' di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici"[28].

Restano, di conseguenza, esclusi dall'applicazione del GDPR i c.d. dati anonimi[29], quelle informazioni che non si riferiscono a una persona identificata o identificabile, o i dati personali "resi anonimi" in modo tale che l'interessato non sia o non sia più identificabile[30]. Per questi dati non vigerà la disciplina prevista in materia di informativa, consenso[31], obblighi ulteriori per il titolare del trattamento come valutazione del rischio

[28] Rispetto al requisito dell'identificabilità *The Article 29 Working Party*, nel citato parere non vincolante 4/2007 sul concetto di dati personali (vedi sopra nota…) sostiene che sia strettamente legata alla valutazione del "se" i mezzi d'identificazione abbiano o meno "ragionevoli probabilità di essere utilizzati" dal responsabile del trattamento "o da qualsiasi altra persona" locuzione spesso interpretata nel significato di "chiunque". Al tempo stesso, il WP29 chiarisce che una "possibilità puramente ipotetica" di identificazione è insufficiente per soddisfare il criterio della "ragionevolmente probabile". Per valutare questa possibilità, invece, "tutti i fattori in gioco" dovrebbero essere considerati, fattori quali le finalità del trattamento, il costo del processo di identificazione, lo stadio della tecnologia, le misure poste in atto dal responsabile del trattamento per evitare l'identificazione, il rischio concreto di una falla tecnica nel sistema.

[29] Peraltro alla luce della dimensione "sociale" e "relazionale" del diritto alla privacy, la dottrina aveva avuto già modo di criticare la scelta di svincolare il dato anonimo (o anonimizzato) da ogni controllo, rilevando come anche il trattamento dei dati anonimi potesse risultare lesivo degli interessi dei singoli, in quanto membri di una comunità, potendo essere alla base di scelte inerenti un determinato gruppo etnico o linguistico o, ancora, potendo condizionare decisioni politiche ed economiche. S. RODOTÀ, *La privacy tra individuo e collettività* (1974), in Id., *Tecnologie e diritti*, Bologna, 1995, p. 29; cfr. anche P.M. VECCHI, Art. 4, in C.M. BIANCA, F.D. BUSNELLI, *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 ("Codice della privacy")*, Padova, 2007, p. 53.

[30] Si parla di "anonimizzazione" esclusivamente quando il "titolare" del trattamento non è in grado in nessun modo di risalire al dato specifico di un interessato perché non possiede più, o non ha mai posseduto, le informazioni complete. Da non confondere con la "pseudonominizzazione" (art. 4, par. 5 GDPR) che è una tecnica di cifratura che consiste nel conservare i dati in una forma che impedisce l'identificazione della persona senza l'utilizzo d'informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati non siano attribuiti a una persona fisica identificata o identificabile.

[31] Sulla rilevanza del consenso, già nel vigore della vecchia disciplina, S. PATTI, *Consenso, sub art. 11,* in C.M. BIANCA, F.D. BUSNELLI (a cura di), *Tutela della privacy (l. 31 dicembre 1996, n. 675)*, in *Nuove leggi civ. comm*., 1999, p. 360; Id. *Riv. dir. civ*., 1999, II, p. 457 ss., nonché in *Commento all'art. 23, La protezione dei dati personali*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *Commento al D. lgs. 30 giugno 2003, n. 196 ("Codice della Privacy*), Padova, 2007, 543 ss.; V. CUFFARO, *Il consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO, (a cura di) *La disciplina del trattamento dei dati personali*, Torino, 1997, p. 201 ss.

d'impatto, controlli, responsabilità e sanzioni; la regola generale, salvo quanto espressamente disposto dal regolamento 1708 del 2018 [32], sarà il loro libero utilizzo.

Il "criterio" della ragionevole probabilità d'identificazione che restituisce la norma appare, tuttavia, intrinsecamente dipendente dal "contesto" [33] in cui il dato viene immesso e la stessa considerazione dei dati come "personali", di conseguenza, risulta essere connotata da un implicito tratto di dinamicità [34]: ciò che intendiamo rimarcare è che lo stesso insieme di dati può non essere identificabile all'inizio del trattamento, o dal punto di vista del responsabile del trattamento, in ragione degli strumenti a sua disposizione, ma può divenire tale in seguito, quando le circostanze "tecnologiche" cambiano, o esserlo sempre stato, dalla prospettiva di un altro soggetto.

Non solo. L'enorme numero di dati (*rectius*: informazioni) che ciascuno di noi è disposto a condividere quotidianamente nei diversi sistemi interattivi, raccolti in banche dati e scambiati e combinati ai più diversi fini – pubblicitari, di pubblica sicurezza, etc. – fanno si che rispetto a ogni singolo individuo sia possibile raccogliere un tale numero di elementi identificativi da rendere, da un lato, astrattamente possibile la riconnessione di ciascun dato a una persona [35] e, dall'altro, quanto mai complesso e costoso un efficiente processo di anonimizzazione [36].

---

[32] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[33] P. SCHWARTZ, D. SOLOVE, *'The PII Problem*., cit., 1848.

[34] N. PURTOVA, *The law of everything*., cit. p. 43 ss.

[35] Uno studio dell'Istituto di Tecnologia di Cambridge (il MIT) pubblicato sulla rivista Science nel 2014 conferma che attraverso l'estrazione e l'aggregazione di dati non identificativi sia possibile risalire all'identità di una persona, de-anonimizzarla. Lo studio si è basato sull'analisi di transazioni con carta di credito effettuate nel corso di tre mesi, analisi dalla quale è stato possibile monitorare la spesa di 1,1 milioni di persone in 10.000 negozi in un unico paese. La banca non ha fornito nomi, numeri di carte di credito, indirizzi di negozi e persino gli orari esatti delle transazioni, ma solo i metadati: gli importi spesi, il tipo di negozio – ristorante, palestra o negozio di alimentari, etc. – e un codice che rappresenta ogni persona. Poiché il modello di spesa di ogni individuo è unico, i dati hanno rilevato una "unicità" molto elevata, rendendoli adatti a quello che è stato definito un "attacco di correlazione". Per poter risalire all'identità di ciascun soggetto è stato sufficiente mettere in relazione i metadati con le informazioni sulla persona provenienti da fonti esterne. Cfr. J. BOHANNON, *Credit Card Study Blows Holes in Anonymity, in Science*, 2015, p. 468 ss.

Già un anno prima, nel 2013, un altro gruppo di ricerca del MIT era riuscito a risalire all'identità di una cinquantina di partecipanti al progetto internazionale "*1000 Genome*" (un progetto che ha come obiettivo scientifico lo studio e l'analisi dettagliata del genoma umano, al fine di offrire alla comunità scientifica uno strumento sulla variabilità genetica mettendo a disposizione una banca dati ad accesso aperto) a partire dai campioni di DNA anonimizzati e resi disponibili online per fini di ricerca. Anche in questo caso, attraverso un algoritmo è stato possibile re-identificare i soggetti combinando i dati genetici che si ritenevano anonimi con altre informazioni contenute in banche dati liberamente accessibili o con dati altrimenti reperibili online. Cfr. M. GYMREK, A.L. MCGUIRE, D. GOLAN, E. HALPERIN, Y. ERLICH, *Identifying personal genomes by surname inference*, in *Science*, vol. 339, 2013, p. 321 ss.

[36] In argomento G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e big data*, cit., p. 474.

Del resto è evidente che, come base per la creazione di valore, i dati possiedono, perlomeno in linea di principio, un valore economico che aumenta con l'aumentare della possibilità di identificare gli utenti anche individualmente. Sebbene, infatti, per la taratura dei modelli algoritmici possono essere utilizzati dati resi anonimi, così come per l'ottimizzazione meramente interna dei processi, tuttavia, la pubblicità personalizzata, così come la definizione granulare di prodotti e prezzi e in parte anche il commercio di dati necessita normalmente di dati personali, perché altrimenti sarebbe preclusa l'associazione con un potenziale cliente concreto.

Se, dunque, come sostenuto dal WP29, i dati personali possono essere qualificati come "anonimi", solo se "l'anonimato è irreversibile", oggi non appare ragionevolmente possibile definire un dato veramente "anonimo" [37].

2.1 – Per comprendere a pieno la portata della definizione di "dati personali" che, come detto, determina in larga misura il campo di applicazione materiale della legge sulla protezione dei dati, è altresì interessante analizzare la giurisprudenza della Corte di Giustizia Europea.

La Corte si è occupata del significato del concetto di "identificabilità" nella Causa *Breyer* [38] ove ha adottato un approccio di ampio respiro, estendendo la nozione di dati personali (ai fini della applicazione della direttiva 95/46/CE, non essendo ancora entrato in vigore il GDPR) anche agli IP (*Internet Protocol*) dinamici [39].

La controversia riguardava il sig. Breyer, attivista tedesco, membro del Parlamento dello Stato Federato di Germania, il quale, dopo aver visitato alcuni siti web accessibili al pubblico delle istituzioni federali tedesche, aveva esperito un'azione inibitoria nei

---

[37] Come noto i pareri del WP29 – organo consultivo – non hanno valore legale; la Corte di Giustizia Europea non li cita mai, ma possono tuttavia avere un'influenza indiretta su come il concetto di "dati personali" si sviluppa nella giurisprudenza, se non in termini di risultati sostanziali, sicuramente fornendo un elenco di questioni da tenere in considerazione.

[38] Corte di Giustizia UE, II, causa C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 ottobre 2016. La sentenza è stata commentata da A. B. SUMAN, *Indirizzi IP dinamici e Cybersicurezza: la conservazione dei "dati personali" degli utenti da parte dell'Internet provider nel caso Breyer*, in *Orientamenti della Corte di giustizia dell'Unione Europea in materia di responsabilità civile*, a cura di G. ALPA E G. CONTE, Torino, 2018, p. 119 ss. nonché da D. MARRANI, *Dati personali e cybersicurezza: la decisione Breyer della Corte di Giustizia*, in *http://www.sidiblog.org/2017/04/11/dati-personali-e-cybersicurezza-la-decisione-breyer-dellacorte-di-giustizia/, 17 aprile 2011*.

[39] Gli IP dinamici sono rappresentati da una sequenza numerica assegnata in maniera temporanea dai fornitori di accesso alla rete ai loro clienti.

confronti della Repubblica federale di Germania per ottenere la cancellazione degli IP dinamici che egli aveva utilizzato per la consultazione dei succitati siti internet. L'istituzione si difendeva opponendo il suo diritto a registrare e conservare tali indirizzi al fine di prevenire possibili attacchi informatici. La domanda veniva rigettata in primo grado e parzialmente accolta in appello, per essere poi impugnata dinanzi alla *Bundesgerichtshof* che decideva di sottoporre alla Corte di Giustizia Europea alcune questioni pregiudiziali, prima fra tutte la possibilità di estendere agli indirizzi IP dinamici la nozione dati personali, quesito al quale la Corte offre una risposta affermativa.

In una precedente occasione, nella causa *Scarlet Extended*[40], la Corte aveva ritenuto che gli indirizzi IP statici fossero dati personali perché, proprio in quanto "statici", ossia invariabili, consentono al fornitore di servizi internet di identificare con precisione gli utenti[41]. Tuttavia, nel caso *Breyer* la controversia ha a oggetto indirizzi IP dinamici, indirizzi che cambiano ogni volta che c'è una nuova connessione internet, e pertanto non consentono al gestore del sito (l'internet service provider) di stabilire un collegamento tra un determinato computer associato al collegamento fisico e la connessione internet. Solo il fornitore di accesso alla rete (l'*internet access provider*) dispone delle informazioni aggiuntive necessarie per identificarlo. Il gestore del sito – nel caso di specie la Repubblica Federale di Germania – pur registrando gli indirizzi IP degli utenti, non sarebbe stato in grado di risalire all'identità del soggetto utilizzatore della rete, dovendo,

---

[40] Corte di Giustizia UE, causa C-70/10 *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Editeurs SCRL* (SABAM), 24 novembre 2011, di cui si può leggere una nota di commento di V. KEYDER in *https://www.cambridge.org/core/journals/international-legal-materials/article/european-court-of-justice-scarlet-extended-sa-v-societe-belge-des-auteurs-compositeurs-et-editeurs-scrl-sabam/F1BCA4E18E72AA6910FAE3296697156*F.

[41] La classificazione degli *Internet Protocol* (IP) quali dati personali ha determinato l'insorgere di un conflitto tra tutela della privacy e tutela dal diritto d'autore in tutte quelle ipotesi in cui al fine di tutelare le opere d'autore o d'ingegno reperibili on-line da illeciti "scarichi" (si pensi, ad esempio, a brani musicali) si renda necessario recuperare dagli Internet Provider gli indirizzi IP di coloro che possano compiere tale attività illecita. Il conflitto di cui si tratta è stato oggetto di alcune pronunce del Tribunale di Roma nell'anno 2006, note sotto il nome di caso *Peppermint* e di un apposito provvedimento del nostro Garante della Privacy del febbraio 2008, n. 1495246. La società discografica Peppermint per tutelare le proprie opere di ingegno nella distribuzione on line – nella specie file musicali – aveva svolto, attraverso una società informatica svizzera, un sistematico monitoraggio delle reti peer to peer (P2P). Tramite l'utilizzo di software specifici, le società avevano individuato numerosissimi indirizzi IP relativi a utenti ritenuti responsabili dello scambio illegale di file: erano poi risaliti ai nomi degli utenti, anche italiani, al fine di potere ottenere un risarcimento del danno. Il Garante ha ritenuto illecita l'attività svolta dalle società per violazione di una serie di disposizione del codice della privacy ed in particolare dei principi di finalità, di trasparenza e correttezza. Per un'ampia e accurata ricostruzione delle problematiche inerenti al tema qui accennato, si veda il contributo di A. M. GAMBINO, R. PETTI, *Privacy e proprietà intellettuale*, in *Privacy digitale*, a cura di E. TOSI, Torino, 2019, p. 229 ss.

per far ciò, ottenere le informazioni in possesso del fornitore di servizi internet. L'indirizzo IP dinamico non costituisce, dunque, un'informazione "relativa a una persona fisica identificata", poiché l'identità del proprietario o di un altro utente di un computer recante l'indirizzo IP non è rivelata direttamente. La questione centrale posta alla Corte riguarda il se tale indirizzo IP possa costituire, tuttavia, un'informazione "relativa a una persona fisica identificabile", potendo i dati supplementari necessari per l'identificazione del visitatore del sito web essere reperiti da gestore del sito presso il fornitore di accesso alla rete.

L'avvocato generale nelle sue conclusioni – affermative – si appella al Considerando 26 della direttiva 95/46 (all'epoca in vigore) ove si afferma che, per determinare se una persona è identificabile "è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare la persona". I giudici della Corte accolgono l'argomentazione sostenendo che nel caso di specie il passaggio d'informazioni sia "ragionevole" nel senso di relativamente facile, non particolarmente costoso e non vietato dalla legge. La Corte, così statuendo, afferma espressamente, per la prima volta che, perché un determinato dato sia qualificato come dato personale, non è necessario che tutte le informazioni che consentono l'identificazione siano nelle mani di un unico soggetto.

La nozione di dati personali contenuta nel nuovo GDPR ha fatto propria questa evoluzione interpretativa, lì dove la nozione di dato personale appare più dettagliata sia nella specificazione del concetto d'"identificabilità"[42], che nelle indicazioni contenute al considerando 30[43].

Un altro caso, deciso nel dicembre 2017, è particolarmente significativo per la normativa europea sulla protezione dei dati e per la definizione del concetto di "dati personali" in quanto fornisce un'interpretazione estensiva di cosa si debba intendere per "qualsiasi informazione riguardante una persona fisica": si tratta del caso *Nowak*[44]. Il sig. Nowak,

---

[42] Art. 4 (1) GDPR: "'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 uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale".

[43] Considerando 30 GDPR "Le persone fisiche possono essere associate a identificativi online prodotti da dispositivi, dalle applicazioni, dagli strumenti e dai prodotti utilizzati, quali gli indirizzi IP, marcatori temporanei (cookies) o identificativi di altro tipo, quali i tag di identificazione e radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

[44] Corte di Giustizia UE, causa C-434/16, *Peter Nowak v Data Protection Commissioner*, 20 dicembre

candidato a una prova di esame, aveva chiesto, sulla base del diritto di accesso ai propri dati personali [45], di poter prendere visione della prova scritta dell'esame che non era riuscito a superare.

L'Istituto presso il quale si era svolta la prova di esame aveva, tuttavia, negato l'accesso, avendo ritenuto che la prova d'esame non contenesse dati personali e non rientrasse, quindi, nel campo di applicazione della legge sulla protezione dei dati. Il sig. Nowak aveva, conseguentemente, presentato un reclamo formale all'*Irish Data Protection Commissioner* (DPC), il quale, a sua volta, aveva ritenuto che il testo dell'esame non contenesse dati personali e che la richiesta fosse stata legittimamente respinta. Dopo vari ricorsi, la Corte Suprema Irlandese aveva deciso di rinviare alla Corte di Giustizia europea il compito di stabilire se le risposte scritte fornite da un candidato a una prova d'esame e i commenti degli esaminatori in merito a tali risposte possano rientrare nella definizione di "dati personali" ai sensi della normativa sulla privacy. Sia l'avvocato generale nelle sue conclusioni che la Corte hanno risposto positivamente.

La CGUE ha ritenuto che le risposte scritte fornite da un candidato e le osservazioni dell'esaminatore in merito a tali risposte costituiscono "informazioni relative a quel candidato" e che sono, quindi, "dati personali". La Corte ha precisato, in particolare, che un candidato all'esame è una persona fisica che può essere identificata, sia direttamente attraverso il suo nome, sia indirettamente attraverso il suo numero d'identificazione, per la prova d'esame. Non ha alcuna importanza se l'esaminatore possa o meno identificare il candidato nel momento in cui corregge e segna il testo. Come nel caso di *Breyer*, per poter trattare le informazioni come dati personali, non è necessario che tutte le informazioni che consentono l'identificazione della persona interessata siano nelle mani di una sola persona. Era indiscusso che, anche nel caso in cui l'esaminatore non fosse a conoscenza dell'identità del candidato al momento della correzione della prova d'esame, l'istituto disponeva delle informazioni necessarie per identificare il candidato (attraverso il suo numero di identificazione).

Rispetto all'uso dell'espressione "qualsiasi informazione" nella definizione del concetto di dati personali la Corte, altresì, afferma che tale definizione non riguarda solo le informazioni sensibili o private, ma potenzialmente comprende tutti i tipi d'informazioni, oggettive e anche soggettive, espresse sotto forma di pareri e valutazioni, purché

2017, di cui si può leggere un commento di K.I. PODSTAVA, *Peter Nowak v Data Protection Commissioner: You Can Access Your Exam Script, Because It Is Personal Data*, in *European Data Protection Law Review*, 4, 2018, p. 252 ss.

[45] L'art. 15 del GDPR regolamenta in modo molto dettagliato il diritto di accesso ai propri dati personali.

"riguardino" la persona interessata. Tale condizione è soddisfatta quando l'informazione, per il suo contenuto, scopo o effetto, è collegata a una persona particolare. Le risposte scritte presentate da un candidato a un esame costituiscono, pertanto, informazioni che gli sono collegate in quanto persona. Il contenuto di queste risposte riflette l'estensione delle conoscenze e delle competenze del candidato in un determinato settore e, in alcuni casi, le sue capacità intellettive, le sue capacità di ragionamento, etc. Lo scopo della raccolta di tali risposte è quello di valutare le capacità professionali del candidato e l'idoneità all'esercizio della professione in questione. Anche i commenti dell'esaminatore costituiscono informazioni relative al candidato, in quanto riflettono l'opinione o la valutazione dell'esaminatore sulle prestazioni individuali del candidato all'esame e sulle sue conoscenze e competenze nel settore interessato. Gli interessati godono pertanto, rispetto a tali prove, del diritto di accesso e di rettifica dei dati, ma la portata di tale diritto è determinata in funzione dello scopo per il quale i dati sono stati raccolti (e quindi, ad esempio, non per la correzione di risposte "errate").

Da ultimo, ma solo in ordine di tempo, si segnala la decisione sul Caso *Planet49*[46] in cui la Corte di Giustizia europea, nel ritenere necessario il consenso degli utenti alla raccolta dei dati da parte dei fornitori di servizi e prodotti digitali mediante l'utilizzo dei *cookies* e *tracking tools*[47], ha affermato che il consenso degli utenti all'istallazione di detti dispositivi è necessario indipendentemente dal fatto che le informazioni memorizzate mediante l'utilizzo degli stessi riguardino o meno dati qualificabili come "dati personali". La Corte, sollecitata – tra le altre cose – a chiarire se le informazioni memorizzate dai cookies possano essere qualificate (o meno) come dati personali e se ciò possa comportare delle differenze rispetto alla gestione di tali dispositivi, ha affermato che

[46] Grande Sez., C-673/17 del 1° ottobre 2019.

[47] Il caso riguardava la *Planet49*, una società tedesca che aveva indetto sul suo sito web una lotteria per partecipare alla quale era richiesto di inserire il proprio nome e indirizzo. Sotto i campi di input per l'indirizzo erano due serie di caselle di controllo. La prima casella di controllo non era stata pre-spuntata, e, ove spuntata dal partecipante, era destinata a consentire l'invio al partecipante di offerte commerciali da parte di alcuni sponsor. La seconda casella di controllo era, invece, pre-spuntata ed era destinata a consentire che fossero installati dei cookies sul dispositivo dei partecipanti allo scopo di fornire annunci mirati. Secondo il regolamento della lotteria, la partecipazione era possibile solo se il partecipante avesse spuntato almeno la prima casella di controllo. La *Bundesverband* (Federazione delle organizzazioni tedesche dei consumatori) ha avviato un procedimento giudiziario contro Planet49, sostenendo che le dichiarazioni di consenso di quest'ultima utilizzate per la lotteria non soddisfacevano i necessari requisiti di consenso informato e libero. La causa è stata deferita alla Corte federale di giustizia tedesca, che l'ha poi deferita alla Corte di giustizia dell'Unione europea, chiedendo orientamenti sull'interpretazione di alcune disposizioni della direttiva *e-Privacy* (direttiva 2002/58/CE, v. nota succ.), della direttiva sulla protezione dei dati (direttiva 95/46/CE, la "DPD") e del regolamento generale sulla protezione dei dati (regolamento 2016/679/UE, il "GDPR").

"l'installazione dei cookie … rientra nel trattamento di dati personali", basandosi sulla considerazione che l'articolo 5, paragrafo 3, della direttiva 2002/58 [48], nel far riferimento all'"archiviazione di informazioni" e all'"accesso a informazioni già archiviate", senza qualificare tali informazioni né precisare che queste debbano essere dati personali, "mira a proteggere l'utente da qualsiasi ingerenza nella sua vita privata, indipendentemente dal fatto che detta ingerenza riguardi o meno dati personali". Una interpretazione avvalorata, a detta della stessa Corte, dal considerando 24 della direttiva 2002/58, secondo il quale "qualsiasi informazione archiviata nell'apparecchiatura terminale degli utenti di reti di comunicazione elettronica fa parte della sfera privata dell'utente, che deve essere tutelata ai sensi della Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali. Detta tutela si applica a qualsiasi informazione archiviata in tale apparecchiatura terminale, indipendentemente dal fatto che si tratti o meno di dati personali" ed è volta, in particolare, come risulta dal medesimo considerando, "a tutelare gli utenti dal rischio che identificatori occulti o altri dispositivi analoghi si introducano nell'apparecchiatura terminale dell'utente a sua insaputa" [49].

3. – Quanto osservato nei paragrafi che precedono rende sufficientemente chiaro del perché, nella comunità scientifica che si occupa di protezione dei dati personali, la discussione su quale sia l'ambito di applicazione della definizione di "dato personale" e, soprattutto, quale possa essere il futuro di questa iconica locuzione [50] è, da tempo, avviata [51].

---

[48] La Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, meglio nota come direttiva e-Privacy, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, modificata dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009. La direttiva dovrebbe essere modificata dal nuovo Regolamento e-Privacy, ancora in fase di negoziazione.

[49] Ragione per cui la Corte afferma che "l'articolo 2, lettera f), e l'articolo 5, paragrafo 3, della direttiva 2002/58, letti in combinato disposto con l'articolo 2, lettera h), della direttiva 95/46, nonché con l'articolo 4, punto 11, e l'articolo 6, paragrafo 1, lettera a), del regolamento 2016/679, non devono essere interpretati in modo diverso a seconda che le informazioni archiviate o consultate nell'apparecchiatura terminale dell'utente di un sito Internet costituiscano o meno dati personali, ai sensi della direttiva 95/46 e del regolamento 2016/679".

[50] R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0*, cit., p. 165 ss.

[51] P. OHM, *Broken promises of privacy*, cit., p. 1701; E. GRATTON, *If Personal Information Is Privacy's Gatekeeper, then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information*, in *Alb. L.J. Sci. & Tech*., 24, 2013, 105; B.J. KOOPS, *The Trouble with European Data Protection Law*, *4 International Data Privacy Law*, 2014, p. 4 ss.; P SCHWARTZ, D. SOLOVE, *Reconciling Personal Information in the United States and European Union*, 102 *California Law Review* 877, 2014.

La definizione di dato personale, quale offerta dal GDPR, è messa in crisi da un processo tecnico che travolge la distinzione fondamentale su cui il regolamento si basa, quella fra dati personali e dati non personali (o anonimi o anonimizzati), distinzione che si attua e si realizza proprio attraverso la categoria dell'identità, nella misura in cui è proprio l'identità della persona che segna il confine tra dati per i quali opera un certo regime – i dati personali, appunto – e quelli per i quali ne opera un altro – i dati anonimi.

Se la tecnologia si sta rapidamente approssimando alla perfetta identificabilità delle informazioni, di tutte le informazioni, anche quelle astrattamente qualificabili come anonime [52]; se gli sviluppi nei processi di analisi e utilizzazione dei dati stanno trasformando tutto in "informazioni" che, interconnesse fra loro in ambienti sempre più "intelligenti" [53], possono agevolmente essere ricondotte a una persona o a un gruppo di persone, con molteplici finalità; se, dunque, nell'era dell'internet degli oggetti, della *data-identification*, dell'analisi avanzata dei dati e del processo decisionale basato sui dati, lo stesso rapporto tra informazione e persona appare ormai sempre più problematico nel senso che ogni informazione è potenzialmente riferibile a una persona [54]; se tutto questo è vero, allora la distinzione fra dati personali e dati anonimi è destinata – inevitabilmente – a venir meno e comunque a ridimensionarsi, e con essa, non solo i due pilastri su cui si fonda il sistema di tutela del GDPR, ma più in generale, il sistema di tutela della stessa identità personale.

In primo luogo – si osserva [55] – un insieme di regole di protezione complesso come

---

[52] P. OHM, *Broken promises of privacy*, cit., p. 1701.

[53] Cfr. D. WEINBERGER, *La stanza intelligente*, Torino, 2012, *passim*.

[54] Quella di dato personale diventa una definizione – così come è soggetta ad allargarsi a dismisura per essere applicata ad un numero crescente ed esponenziale di situazioni – destinata nel lungo termine a perdere ogni utilità rispetto al fine cui è preposta, cfr. N. Purtova, *The law of everything*, cit., p. 75. L'autrice ritiene che i rischi maggiori di tale tendenza interpretativa siano pericolosi a lungo termine, più che a breve termine, e ciò per due ordini di ragioni: da un lato perché la tecnologia non ha ancora raggiunto un livello tale da poter effettivamente "trasformare" ogni informazione in una "informazione personale" (anche se il traguardo non appare così lontano) e secondariamente perché nonostante la portata ampia della definizione, alcune "informazioni" che potrebbero essere considerate dati personali – e quindi azionare la disciplina – ancora non sono riconosciute come tali. Ciò perlopiù avviene a causa della mancanza di consapevolezza da parte dei responsabili del trattamento circa l'esatto significato della definizione di "dati personali", ai sensi della legge sulla protezione dei dati. Così, ad esempio gli scienziati che si occupano dei dati e dei processi di anonimizzazione partono dal presupposto che un determinato progetto di analisi dei dati da loro pianificato abbia un certificato di protezione dei dati "pulito", poiché i dati in questione sono criptati o privi di identificatori e quindi "non contengono dati personali". I giuristi possono rispondere che se i ricercatori hanno o è ragionevolmente probabile che abbiano accesso alla chiave di cifratura o agli identificatori, l'insieme di dati in questione è stato oggetto di "pseudonimizzazione" piuttosto che di "anonimizzazione", e l'insieme dei dati resta, perciò, soggetta alla legge sulla protezione dei dati.

[55] N. PURTOVA, *The law of everything*, cit., p. 75.

quello previsto dal GDPR, ove deputato a disciplinare una gamma di situazioni sempre più ampia, in ragione della sempre più "elastica" definizione di dati personali (che avrebbe, invece, lo scopo di delimitarne l'operatività), rischia di non essere a lungo termine sostenibile e ritorcersi a sfavore di chi lo promuove, perché i titolari del trattamento, invece di impegnarsi in una valutazione "significativa" dei rischi, saranno spinti a creare solo l'apparenza formale di conformità [56]. Contestualmente l'ampliarsi a dismisura del campo operativo dei rimedi, specie quelli aquiliani, dovuto al fatto che molti trattamenti fin qui tenuti al riparo dal consenso preventivo e da altre condizioni di liceità potrebbero diventare illeciti, nello sbilanciare il delicato equilibrio tra tutela del diritto individuale alla protezione dei dati e diritto al trattamento e alla libera circolazione, rischierebbe di compromettere significativamente la libertà di iniziativa economica.

Ed infatti l'abbandono della distinzione tra dati personali e non personali in favore di un sistema di tutela disancorato dalla qualificazione del dato, in cui ogni trattamento di dati richiederebbe probabilmente le procedure di rilascio del consenso o altre basi di trattamento, potrebbe far scattare in funzione compensativa un sistema di protezione modulabile, calibrato su una matrice di "rischio del danno", idonea ad introdurre una metodologia flessibile di valutazione dei dati e di conseguente "dosaggio" della performance di trattamento.

Ma questo possibile sistema comporterebbe, di fatto, l'abbandono dell'identità come di strumento di tutela per quanto imperfetta dai "poteri forti" – i *players* dei *big data* – che sarebbero lasciati liberi di "giocare" senza dover osservare le regole della privacy, se non sulla base di un giudizio prognostico con cui si finisce per delegare al soggetto che intende trattare i dati la scelta di applicare o meno, in regime di discrezionalità, la relativa disciplina [57].

Prescindendo, in questa sede, da altre valutazioni sulla concreta possibilità di individuare valide alternative all'attuale sistema di protezione del dato personale, ci limitiamo a qualche riflessione di più ampio respiro.

L'identità, come situazione giuridica protetta, presuppone e si fonda sul potere individuale di disegnare, sulla base della volontà, la propria sfera personale perché, dal punto di vista giuridico, è "la volontà soggettiva la regola di conformazione dell'identità personale" [58]. La scelta del legislatore europeo è stata, non a caso, quella di garantire protezio-

---

[56] Basterà munirsi di "etichette di certificazione", saranno indicati "marchi di fiducia", "surrogati" di veri e propri processi di valutazione dei rischi.

[57] R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0*, cit., p. 176 ss. alla quale si rinvia per una più trattazione di sistemi alternativi sino ad ora proposti.

[58] D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 384.

ne al "dato personale" riconoscendo al singolo il potere di mantenere il controllo sul 'frammento d'identità', per permettere a ciascun individuo, così facendo, di determinare le modalità di costruzione della propria sfera privata [59].

Ma se – come sembra – la categoria del dato personale si dovesse ampliare sino a ricomprendere tutte le informazioni – senza esclusioni – che ciascuno è in grado di fornire, anche in forma anonima [60], ovvero se – come suggeriscono alcuni – la sfera informazionale e quella identitaria di ciascun individuo dovessero finire sempre e comunque per avere il medesimo contenuto [61], senza che sia più possibile non solo per i terzi, ma anche per il diretto interessato, distinguere (e decidere) tra ciò che rientra nella propria sfera privata e ciò che invece ne resta escluso [62], tutto ciò potrebbe determinare l'insorgere di talune contraddizioni non solo nelle modalità di tutela, ma anche in quelle di esercizio dei diritti individuali, che dovrebbero perciò essere oggetto di un ripensamento.

Più in particolare, il diritto alla protezione dei dati personali è definito come libertà nella Carta dei diritti fondamentali dell'Unione europea, una "libertà" che con il diffondersi delle nuove tecnologie assume rilevanza e connotati diversi: l'effettivo esercizio del diritto di autodeterminazione informativa dovrebbe, infatti, configurarsi come espressione della libertà del singolo di "controllare" i propri dati, in positivo come in negativo, pretendendo che non tutti i dati che promanano dalla propria sfera individuale siano sempre e comunque ad essa ricondotti, preservando – per questa via – la possibilità per il singolo di determinare (in negativo) la propria identità.

Ribaltando la prospettiva, allora, assume rilievo il diritto all'anonimato che, ove correttamente valorizzato dall'ordinamento, si palesa un diritto a contenuto non più esclusivamente negativo, che si risolve nel diritto a non rivelarsi, ma una modalità di controllo della proiezione della propria identità [63], che implica la non riconducibilità del dato alla

---

[59] S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice della Privacy*, in *Eur. dir. priv*., 2004, p. 2 ss.

[60] G. FINOCCHIARO, voce *Anonimato*, in *Dig. disc. priv*., Sez. civ., 2010, (banca dati Leggi d'Italia).

[61] L. FLORIDI, *La quarta rivoluzione*, Milano, 2014, p. 71 ss. Partendo dalla constatazione che "noi siamo le nostre informazioni", Floridi sostiene che ogni violazione della "privacy informazionale" debba essere considerata una forma di aggressione rivolta all'identità del singolo: quella che Floridi definisce l'"interpretazione autofondativa della privacy" suggerendo che la sfera informazionale e quella identitaria di ciascun individuo abbiano il medesimo contenuto, che siano i due lati della stessa medaglia, con ciò arrivando ad elevare a rango di diritto fondamentale non più, o non solo, la protezione del dato personale ma la stessa "identità personale informazionale", "cosicché tutto ciò che è fatto alle nostre informazioni è fatto a noi e non a ciò che possediamo".

[62] Così, per esempio, si potrebbe ancora immaginare di esprimere un'opinione in forma anonima?

[63] Cfr. G. FINOCCHIARO, voce *Anonimato*, cit.

persona che lo ha prodotto (e come tale può costituire anche un valido strumento di protezione della persona da forme di controllo più pervasive favorite dalle nuove tecnologie, quali profilature e schedature [64]).

Sebbene la riconducibilità di tutti i dati al suo autore, grazie agli sviluppi della tecnica, potrebbe apparentemente garantire a quest'ultimo una maggior tutela, in realtà l'intero processo finisce con il trasformarsi in un boomerang destinato a colpire – rischiando di comprometterle – due situazioni giuridiche consolidate. La prima è il diritto all'anonimato, gravemente pregiudicato dal potenziale divenire della persona una scatola di vetro a tutela inflazionata. La seconda è il diritto al trattamento dei dati personali, come "libertà" regolata e vincolata da diversi plessi normativi [65], che sembra destinato ad uscire dal necessario bilanciamento con altri diritti, gravato di limiti e costi che ne pregiudicano un esercizio efficiente (il che è quanto avverrebbe se per ogni categoria di dati il titolare del trattamento dovesse sviluppare una base di legittimazione, il consenso, che la persona non è affatto interessata a dare proprio per evitare di essere identificata).

Si rivela così l'ennesima paradossale contraddizione tra gli esiti che la tecnologia offre alla società e ai regolatori, e la strutturazione poliedrica dei diritti individuali, fin qui costruita intorno all'autodeterminazione individuale e alla libertà d'impresa.

---

[64] Cfr. M. MANETTI, *Libertà di pensiero e anonimato in internet, in Diritto dell'informazione e dell'informatica*, 2, 2014, p. 139 ss.

[65] Si pensi all'interferenza tra disciplina del GDPR e disciplina dell'Antitrust; come evidenziato dalle recenti 3 pronunce dell'AGCM – Provvedimento n. 26596 cv154, *Whatsapp* – Clausole vessatorie e Provvedimento n. 26597 ps1060, *Whatsapp* – trasferimento dati a *Facebook* – dell'11 maggio 2017– e Provvedimento n. 27432 – ps11112, *Facebook* – Condivisione dati con terzi – con cui l'Autorità garante della concorrenza e del mercato (AGCM) ha accertato violazioni del Codice del consumo da parte di WhatsApp, colosso nella gestione di servizi di messaggistica istantanea per smartphone, e da parte di Facebook, colosso dei social network. L'eventuale illegittima raccolta dei dati personali da parte di un professionista-responsabile del trattamento in ragione dell'utilizzo di modalità di raccolta del consenso che possano integrare gli estremi di condotte aggressive e ingannevoli costituisce, oltre che una possibile violazione dei principi in materia di corretto trattamento dei dati personali (prerogativa del Garante per la protezione dei dati personali), anche una violazione delle norme in materia di pratiche commerciali scorrette rispetto alla quale l'Autorità garante della concorrenza e del mercato (AGCM) è altresì legittimata a pronunciarsi. Ma la dimensione della questione travalica, come comprensibile, i confini nazionali: così si veda la decisione del 6 febbraio 2019, *Facebook Inc., Menlo Parc, U.S.A., Facebook Ireland Ltd., Dublin, Ireland, Facebook Deutschland GmbH/Verbraucherzentrale Bundesverband e.V., Berlin con cui la Bundeskartellamt* (omologa tedesca della nostra AGCM) ha proibito a Facebook Inc. (etc.) di subordinare l'utilizzazione del servizio da parte degli utenti residenti in Germania, che utilizzano altresì servizi ricondotti al medesimo gruppo (tipo *WhatsApp*), alla condizione di potersi valere dei dati risalenti all'utente, combinandoli con quelli raccolti in seno alla piattaforma, a meno di un consenso espresso all'impiego di dati relativi ad un uso esterno a *Facebook*. In argomento, per tutti, C. OSTI, R. PARDOLESI, *L'antitrust ai tempi di Facebook*, in *Mercato, Concorrenza, Regole*, 2019, p. 194 ss.