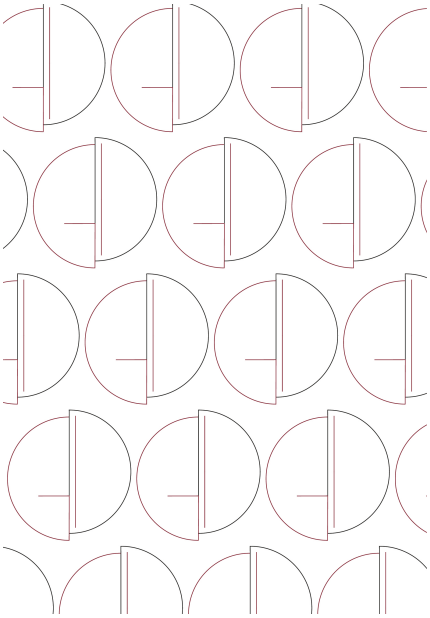
Materiali e documenti

Annuario 2022 Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022 Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo



University Press

Sapienza Università Editrice

Collana Materiali e documenti 90

Annuario 2022
Osservatorio Giuridico sulla Innovazione Digitale

Yearbook 2022
Juridical Observatory on Digital Innovation

a cura di
Salvatore Orlando e Giuseppina Capaldo

SAPIENZA
UNIVERSITÀ EDITRICE
2022

Sapienza Università Editrice
Piazzale Aldo Moro 5 – 00185 Roma

www.editricesapienza.it
editrice.sapienza@uniroma1.it

Iscrizione Registro Operatori Comunicazione n. 11420
Registry of Communication Workers registration n. 11420

ISBN 978-88-9377-256-3

DOI 10.13133/9788893772563

Pubblicato nel mese di dicembre 2022 | *Published in December 2022*

Impaginazione a cura di | *Layout by*: Lucio Casalini e Enzo Maria Incutti

In copertina | *Cover image*: Michela Tenace, *Elaborazione grafica del logo OGID/JODI*, 2022, Archivio personale dell'a.

Indice

2. *Privacy Enhancing Technologies*, trasparenza e tutela della persona nell'ambiente digitale

Alessandro Bernes (Università Ca' Foscari Venezia)

2.1. Le funzioni della tecnologia nell'era digitale

In seguito alla "rivoluzione" condotta dalle nuove tecnologie, per un verso, è reso a molti più semplice e immediato l'accesso ad *Internet* e, in generale, prender parte alla società dell'informazione; per altro verso, con riferimento alla navigazione sul *web*, alla sottoscrizione di servizi digitali, al *download* di contenuti digitali, e via dicendo, gli utenti hanno una scarsa percezione dei rischi legati a dette attività, mentre, al contrario, basano quasi esclusivamente le proprie scelte sulla fiducia, piena e incondizionata, circa la diffusione tra i consociati di quanto loro offerto. Di qui, il problema del c.d. *privacy paradox*, per il quale ciascun individuo tiene molto ad evitare intrusioni non autorizzate nella propria sfera privata, ma al tempo stesso presta poca attenzione alla quantità e alle categorie di dati ad esso riconducibili, raccolti nel momento in cui ci si interfaccia con l'ambiente digitale, soprattutto quando il servizio è fornito "gratuitamente"[1].

[1] Stando a S. BARTH, M. D.T. DE JONG, *The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review*, in *Telematics and Informatics*, 2017(34), p. 1039, «*while many users show theoretical interest in their privacy and maintain a positive attitude towards privacy-protection behavior, this rarely translates into actual protective behaviour* (…) *Although users are aware of privacy risks on the internet, they tend to share private information in exchange for retail value and personalized services*». L'AGCM ha pubblicato, nel 2018, i risultati dell'"Analisi della propensione degli utenti online a consentire l'uso dei propri dati a fronte dell'erogazione di servizi", reperibile *online* all'indirizzo https://www.agcm.it/dotcmsDOC/allegati-news/IC53%20-%20Survey%20primi%20risultati.pdf. In particolare, dal sondaggio, condotto su un campione di utenti di servizi *online*, è emerso che circa 6 utenti su

In realtà, gli individui non sembrano in grado di potere valutare, nella pratica, le conseguenze (future) delle loro scelte in merito all'immissione in Rete di dati personali e, quindi, esercitare un vero e proprio controllo sul loro flusso[2] – anche perché i fornitori di servizi della società dell'informazione dettano unilateralmente la disciplina dei termini e delle condizioni cui gli utenti devono necessariamente adeguarsi, qualora intendano fruire di quanto loro offerto. In questo senso, l'alternativa tra il fornire o no i propri dati per l'utilizzo dei servizi *online* costituisce, invero, una falsa opzione, posto che il mancato accesso a *quel* servizio degenera in una auto-esclusione sociale, nella perdita di benefici ovvero nell'emersione di costi di transazione; ciò che determina un effetto di tipo *lock-in*[3].

Tra le molte ragioni che hanno portato al fenomeno del *privacy paradox*, vi è da chiedersi quale ruolo assuma il *gap* di natura tecnologica, piuttosto che regolamentare in senso stretto[4]. In altre parole, è forse la mancanza di strumenti tecnologici, i quali consentano, in maniera trasparente, la visualizzazione dei dati raccolti, nel tempo, dai servizi della società dell'informazione, ovvero con chi i dati vengono condivisi, ciò che impedisce alle persone di comprendere – ma prima ancora

10 non solo sono consapevoli di generare, con le loro attività *online*, dati utilizzabili per attività di profilazione, ma anche che essi appaiono informati dell'elevato grado di pervasività dei sistemi di raccolta (es. geolocalizzazione, accesso a funzionalità come la rubrica, il microfono e la videocamera) e della possibilità di sfruttamento dei dati da parte delle imprese. Nel complesso è risultato che 4 utenti su 10 sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio. Per l'apparente gratuità delle c.d. *non-monetary transactions*, dove i fornitori di un servizio digitale gratuito vanno a sfruttare commercialmente i dati (personali) resi o generati dagli utenti, si veda C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, p. 61 ss.

2 Sul diritto alla protezione dei dati personali inteso nel senso di controllo da parte del singolo circa le informazioni che lo riguardano, vedi già le precorritrici affermazioni di S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; per l'elaborazione successiva, ID., *Il diritto di avere diritti*, Roma-Bari, 2012. Per una efficace sintesi di una bibliografia oramai sterminata, V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 3 ss.

3 Per tutti, D. J. SOLOVE, *Introduction: Privacy Self-Management and the Consent Dilemma*, in *Harvard Law Review*, 126(7), 2013, p. 1880 ss.

4 Desta perplessità, soprattutto nell'epoca della *Big data analytics*, la possibilità che gli strumenti del diritto possano far fronte, da soli, alla tutela dei dati personali: così A. C. NAZZARO, *L'utilizzo dei* Big data *e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, p. 1239.

di conoscere[5] – i meccanismi di "mercato"[6] dei dati personali o, per meglio dire, la (libera) circolazione delle informazioni nell'ambiente digitale[7]?

Ci si deve domandare, in sostanza, se le tecnologie che permettono il trattamento di dati personali possono venire in supporto anche alla stessa tutela della persona, in modo da riequilibrare, per tale via, l'asimmetria conoscitiva esistente tra chi rende i servizi digitali e coloro che li utilizzano quotidianamente[8]; squilibrio, questo, sia pur esacerbato dal nuovo contesto della Rete, comunque riconducibile a quello, da tempo noto, intercorrente fra professionista e consumatore[9].

Il presente scritto si propone allora di indagare come ci si possa servire della "scelta tecnica" in funzione della protezione dei dati

---

[5] Sulla rilevanza, nell'ordinamento giuridico, della *conoscibilità* piuttosto che della *conoscenza*, vedasi S. PUGLIATTI, *Conoscenza*, in *Enc. dir.*, IX, 1961, p. 45 ss., ove si richiama, peraltro, la postulata correlazione funzionale della volontà (impulso) alla conoscenza e della conoscenza (guida) alla volontà. Più di recente, S. ORLANDO, *Le informazioni*, Padova, 2013, p. 67 ss.

[6] V. ZENO-ZENCOVICH, *Do "Data Markets" exist?*, in *MediaLaws – Rivista di diritto dei media*, 2019, 2, p. 22 ss.

[7] La raccolta di dati personali ma soprattutto la loro analisi e l'estrazione di informazioni inferenziali costituiscono oggi un'operazione confacente a molteplici modelli di *data-driven economy* e di valorizzazione del potere informativo, soprattutto al fine di costruire un profilo utente e giungere sino a predirne i comportamenti. Sul fenomeno della patrimonializzazione dei dati personali, si vedano, per tutti, V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, p. 642 ss., nonché R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2020, p. 760 ss. In giurisprudenza, in merito al noto caso *Facebook vs*. AGCM, si è pronunciato, da ultimo, CONS. STATO, sez. VI, 29 marzo 2021, n. 2631, in *Foro it*, 2021, III, c. 325 ss., con nota di R. PARDOLESI, A. D'AVOLA, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern') parallele convergenti?*

[8] ENISA, *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, 2015, p. 5, ove ci si interroga se i problemi generati dalla tecnologia che rende possibile il trattamento dei dati personali, in particolare per i *digital providers*, possano trovare, oggi, una risposta anche nella stessa tecnologia. Il tema dell'intersezione fra la tecnica giuridica e la tecnica informatica, e dell'apporto fornito dall'una e dall'altra, è una costante della riflessione in tema di *data protection*: sul punto, U. PAGALLO, *Il diritto nell'età dell'informazione. Il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti*, Torino, 2014, p. 285 ss.

[9] L'accostamento della disciplina della protezione dei dati personali alla normativa in tema di tutela del consumatore è stato da tempo evidenziato in dottrina; sul punto, di recente, D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 2019, pp. 2786-2787; F. PIRAINO, *I ''diritti dell'interessato'' nel Regolamento generale sulla protezione dei dati personali*, *ivi*, p. 2789.

personali, al fine di tutelare i diritti fondamentali della persona che si interfaccia con l'ambiente digitale[10]. In particolare, l'attenzione sarà rivolta alle *modalità* attraverso le quali implementare le norme applicabili al trattamento di dati personali, per il tramite di strumenti informatici volti a garantire una maggiore trasparenza delle operazioni e rendere di queste più consapevoli gli individui; allo stesso tempo, attraverso la predisposizione di certune tecnologie da parte dei titolari del trattamento, sembra rafforzarsi l'*effettività* della tutela stessa dei diritti dell'interessato. Ciò dovrebbe determinare, in ultima istanza, un ripensamento, da un lato, quanto ai meccanismi di produzione di norme, almeno in senso formale, diversamente ragionando sui rapporti tra tecnica e diritto[11]; dall'altro lato, guardare al ruolo assunto oggigiorno dai soggetti privati che pongono in essere operazioni con dati personali, quali veri e propri attori della regolazione dei mercati digitali[12].

Il tema indagato si interseca con il noto fenomeno per il quale le principali società tecnologiche – e non solo gli *Internet Service Provider* – hanno assunto oggi, grazie alle economie di scale e agli effetti di rete, il ruolo di *gatekeeper* per l'utilizzo dei servizi offerti dal *Web*: esse esercitano, autolegittimandosi di fatto (d)all'interno del mercato[13], un

[10] Quanto al diritto alla protezione dei dati personali inteso come precondizione al pieno godimento di altri diritti fondamentali dell'uomo, e in ultima istanza della dignità della persona, magistralmente, S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa. Il nuovo codice della privacy*, in *Eur. dir. priv*., 2004, p. 1 ss.

[11] In argomento, G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf*., 2012, p. 831, secondo la quale «oggi l'informazione senza la tecnologia non meriterebbe un discorso a sé, e probabilmente non avrebbe senso (…)». Più in generale, in un dibattito a più voci, N. IRTI, E. SEVERINO, *Dialogo su diritto e tecnica*, Roma-Bari, 2001; L. MENGONI, *Diritto e tecnica*, in *Riv. trim. dir. proc. civ*., 2001, p. 1 ss.; N. IRTI, *Un incompiuto dialogo con Luigi Mengoni*, in *Eur. dir. priv*., 2012, p. 197 ss.

[12] Sul diritto privato in funzione regolativa, di recente, A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, p. 201 ss.; ma cfr. anche V. DE LUCA, *Autonomia privata e mercato telematico nel sistema delle fonti*, Milano, 2004, p. 58, dove si affianca, nell'epoca della globalizzazione, ad una nuova *lex mercatoria* anche una *lex informatica*; in termini simili, G. TEUBNER, *Regimi privati globali. Nuovo diritto spontaneo e costituzione duale nelle sfere autonome della società globale*, in ID., *La cultura del diritto nell'epoca della globalizzazione. L'emergere delle costituzioni civili*, trad. it. a cura di R. Prandini, Roma, 2005, p. 59 ss.

[13] Sui poteri privati che superano la tradizionale parità dei soggetti, fondamentali sono gli studi di C. M. BIANCA, *Le autorità private*, Napoli, 1977; ID., *Ex facto oritur ius*, in *Riv. dir. civ*., 1995, I, p. 787 ss., ove si elaborava una categoria che comunque metteva già in discussione la tradizionale separazione tra pubblico e privato; ma cfr. già W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1963, *passim*. Di recente declinato, con riferimento al nuovo assetto economico-sociale della realtà odierna, si veda il volume di P. SIRENA,

controllo pressoché totale dell'informazione da processare, attraverso meccanismi (per lo più *software*) che consistono nel selezionare, analizzare, riprodurre, estrarre e cancellare l'informazione stessa[14]. Inoltre, le *Big Tech* mostrano di detenere il monopolio delle tecnologie non solo per la raccolta dei dati personali – da riutilizzare poi a fini commerciali – ma sembrano essere addirittura gli unici soggetti in grado di tutelare i diritti dell'interessato, come evidenziato nelle sentenze della Corte di Giustizia dell'Unione Europea in materia di "oblio": qui è stato esplicitamente riconosciuto a *Google* il potere di bilanciare finanche diritti fondamentali[15], da attuarsi, peraltro, mediante il ricorso a strumenti tecnici, quali la de-indicizzazione dei *link* verso le pagine *web* dall'elenco dei risultati mostrati dai motori di ricerca[16].

Eppure, l'emersione di autorità private, e delle soluzioni da esse dettate, è rappresentativa di un fenomeno economico-sociale che non può prescindere dal rispetto delle regole giuridiche, alle quali spetta comunque dare legittimazione ai poteri degli operatori, in funzione non soltanto della regolazione dei mercati, ma soprattutto della tutela dei diritti fondamentali della persona[17]. A tal fine, come si avrà modo

---

A. ZOPPINI (a cura di), *I poteri privati e il diritto della regolazione. A quarant'anni da «Le autorità private» di C.M. Bianca*, Roma, 2018.

[14] Per una panoramica generale, A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2020.

[15] A partire dalla sentenza CGUE, 13 maggio 2014, causa C-131/12, *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, nonché di recente CGUE, 24 settembre 2019, causa C-136/17, *GC e a. contro Commission nationale de l'informatique et des libertés (CNIL)*, confermato anche dall'EDPB, *Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca*, 7 luglio 2020, reperibili *online* all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_it.pdf. Sui rapporti tra diritto all'informazione e diritto all'oblio, per tutti, G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio dopo la sentenza Google Spain*, Roma, 2015.

[16] Di recente, Cass., sez. I, 8 febbraio 2022, n. 3952, in *OneLegale*, ove si rammenta che «attraverso la deindicizzazione l'informazione non viene eliminata dalla rete, ma può essere attinta raggiungendo il sito che la ospita (il cosiddetto sito sorgente) o attraverso altre metodologie di ricerca, come l'uso di parole-chiave diverse»; ma cfr. anche Trib. Milano, 5 settembre 2018, in *Danno e resp.*, 2019, p. 122 ss., con nota di S. BONAVITA, *Deindicizzazione: tecnologie abilitanti ed evoluzione del rapporto tecnologia e diritto*, per il quale il *de-listing* sembra assumere i contorni di una tecnologia applicabile alla tutela di diritti anche diversi dall'oblio.

[17] Nel primo senso, proprio al fine di "responsabilizzare" lo strapotere assunto dai *gatekeeper*, si inserisce, da ultimo, il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale (meglio noto come *Digital Markets Act*); nel secondo, ovviamente, il

di vedere, pare opportuno aggiungere alla norma di fonte eteronoma, l'elaborazione di linee guida, raccomandazioni, *best practices*, certificazioni, codici di condotta, misure di sicurezza e finanche prodotti tecnologici a tutela dei dati personali, che incidano direttamente sui rapporti tra i titolari del trattamento e gli interessati, conformandoli[18]. In ogni caso, al riconoscimento esplicito della libertà di scelta dettata dall'autoregolamentazione interna – declinazione del principio di sussidiarietà orizzontale[19] – è pur sempre necessaria una verifica esterna delle misure tecniche ed organizzative costitutive del trattamento di dati personali (*accountability*[20]), specialmente ad opera delle autorità di controllo[21], favorita dal legislatore in un contesto regolatorio e procedimentalizzato dei mercati digitali[22].

2.2. Le *Privacy Enhancing Technologies*

Nel contesto sopra brevemente illustrato, vengono continuamente ad intrecciarsi la normazione e l'automazione, sicché diritto e tecnologia si trovano legati in un connubio *funzionale*, regolamentare, da un lato, e operativo, dall'altro[23].

Il riferimento va subito ristretto alle c.d. *Privacy Enhancing Technologies* (*PETs*)[24], che già dagli anni '90 del secolo scorso sono state

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, conosciuto anche con l'acronimo GDPR.

[18] G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 234.

[19] P. LAGHI, *Cyberspazio e sussidiarietà*, Napoli, 2015, *passim*.

[20] Per tutti, G. FINOCCHIARO, *Il principio di* accountability, in *Giur. it.*, 2019, p. 2778 ss.

[21] Sul punto, 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"*, in *Dir. inf.*, 2014, p. 805 ss.

[22] Cfr. P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, p. 482.

[23] A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy: privacy by design *e* privacy by default settings, in *Contr. impr./Europa*, 2015, p. 198.

[24] H. VAN ROSSUM, H. GARDENIERS, J.J. BORKING, A. CAVOUKIAN, J. BRANS, N. MUTTUPULLE, N. MAGISTRALE, *Privacy-Enhancing Technologies: The Path to Anonymity*, The Hague, 1995; S. FISCHER-HUBNER, S. BERTHOLD, *Privacy-Enhancing Technologies*, in J. R. VACCA (edited by), *Computer and Information Security Handbook*, 3th ed., Amsterdam, 2017, pp. 759-778.

invocate per realizzare un nuovo approccio alla protezione dei dati personali, noto come *privacy by design*[25] e meglio definibile oggi nella *data protection by design*[26]. Si tratta di un principio che è stato fatto proprio dal Regolamento 2016/679/UE (in avanti, GDPR), posto che, sulla base di una analisi *ex ante* dei rischi e delle circostanze concrete attinenti al trattamento di dati personali, è necessaria non solo la configurazione dei sistemi computazionali idonei a garantirne la legittimità, bensì la predisposizione, sin dal principio, di misure tecniche e organizzative rispondenti alla protezione dei dati personali e ai principi che la governano (art. 25, par. 1, GDPR)[27].

Possono essere considerate *PETs*, in generale, «*systems encompassing technical processes, methods, or knowledge to achieve specific privacy or data protection functionality or to protect against risks to privacy of an individual or a group of natural persons*»[28]. Seguendo la definizione riportata, il concetto è davvero vastissimo e le sue concrete applicazioni innumerevoli. Qui non si intendono sondare le varie tecniche di anonimizzazione (k-*anonimity*, *differential privacy*, etc.) o di elaborazione computazionale distribuite, né indagare sofisticate misure di sicurezza (*homomorphic encryption*)[29]; diversamente, lo sguardo è rivolto verso quelle tecnologie che permettono al titolare del trattamento di implementare, in pratica, il principio generale della *trasparenza* (art. 5, par. 1, lett. *a*, GDPR), nonché garantire un *empowerment* dell'interessato attraverso un effettivo esercizio del potere di controllo dei dati personali, riconducibile al più ampio diritto fondamentale alla loro protezione[30].

---

[25] Per tutti, A. CAVOUKIAN, *Privacy by Design – The 7 Foundational Principles*, August 2009 (revised January 2011), reperibile *online* all'indirizzo https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[26] Come si sottolinea in M. VEALE, R. BINNS, J. AUSLOOS, *When data protection by design and data subject rights clash*, in *Int. Data Privacy Law Rev.*, 2018, p. 2, la mutata espressione non è solo ideologica, dal momento che lo scopo principale del GDPR è la protezione dei dati personali; *amplius*, L. A. BYGRAVE, *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, in *Oslo Law Review*, 4(2), 2017, p. 105 ss.

[27] Per un primo commento, R. D'ORAZIO, *Protezione dei dati* by default *e* by design, in S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, p. 79 ss.

[28] ENISA, *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies Methodology, Pilot Assessment, and Continuity Plan*, 2015, p. 9.

[29] Per una analisi completa, si rinvia a G. D'ACQUISTO, M. NALDI, Big data *e* privacy by design. *Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017.

[30] Sulla differenza tra strategie di *front-end* rispetto a quelle di *back-end*, vedasi A. PRINCIPATO, *Verso nuovi approcci alla tutela della* privacy, cit., p. 200, dove si afferma: «Infatti, nel momento *back-end*, il *design* riguarda i modi di conservazione e trattamento dei dati

Tutto ciò rappresenta un momento essenziale per incrementare altresì la *fiducia* nei mercati digitali, onde evitare reazioni meramente inibitorie da parte degli utenti della Rete, come il rifuggire dal *Web*, in chiara ottica oppositiva[31]. Il compito svolto dalle *PETs* improntate ad una maggiore trasparenza assume, quindi, una posizione di prim'ordine; tant'è che la Commissione europea, di recente, ne ha sottolineato la complementarità rispetto all'attuale quadro normativo, già in vigore o in preparazione, deputato alla regolazione dei traffici nell'era dei *Big Data*[32].

Due precisazioni appaiono necessarie, discorrendo di *PETs*.

La prima, avente carattere preliminare, è che deve essere abbandonata una logica meramente difensiva delle situazioni giuridiche ascrivibili all'interessato. La protezione dei dati personali non si pone, infatti, in posizione conflittuale rispetto all'uso delle tecnologie dell'informazione e della comunicazione e ai loro derivati; al contrario, i diritti del singolo, tra i quali la riservatezza e l'identità personale, vengono costantemente attraversati da altri e diversi interessi, privati o pubblici, che rendono legittime le varie operazioni eseguite con i dati di qualcuno, o perché volontariamente questi si è così determinato, o perché si fa riferimento ad attività necessarie alla stregua di particolari finalità, ritenute meritevoli di tutela, e nel caso specifico prevalenti, perseguite da un soggetto diverso dall'interessato[33].

già acquisiti, e deve assicurare il rispetto di quanto previsto a livello legislativo e contrattuale, assicurando una corretta fruizione dei dati sia a livello di chi tratta i dati sia di parti terze. Il momento *front-end* invece guarda a quanto avviene nel momento in cui l'utente si interfaccia con il servizio fornitogli, a come si acquisiscono i dati personali del soggetto. In quest'ultimo caso, lo scopo deve essere quello di fornire all'utente le necessarie informazioni sui dati che verranno acquisiti e di accrescere il controllo dello stesso su esse».

[31] Si pensi alla ritrosia verso gli *advertising cookies*, con il ricorso a strumenti di *ad-blocking*, operanti come una sorta di "autodifesa" del soggetto dinanzi alla tecnologia adoperata dai servizi digitali, così S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 26.

[32] COMM. EU, *Una strategia europea per i dati*, 19.2.2020 COM(2020) 66 final, p. 22, ove sono definite le "coordinate" fondamentali per le prossime fasi dell'economia dei dati.

[33] Sulla natura relazionale del diritto alla protezione dei dati personali, si veda il *considerando* § 4 del GDPR. In argomento, diffusamente, A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2017, p. 591 ss., ma già F. D. BUSNELLI, *Dalla legge al «codice»: un dilemma, una sfida, un consolidamento normativo, una (imperfetta) razionalizzazione delle tutele*, in C. M. BIANCA, F. D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, I, Padova, 2007, p. XXXIX.

Con l'evolversi della *data-driven economy* e dell'attitudine dell'informazione a fungere da elemento redditizio a molteplici modelli di *business* – ma anche semplicemente considerando la crescente digitalizzazione della vita quotidiana su svariati fronti – non si può pensare che la tutela dei dati personali possa essere lasciata unicamente al singolo, almeno nel senso di pretesa azionabile dinanzi all'autorità, giudiziaria o amministrativa che sia: o perché l'interessato è strutturalmente debole dinanzi all'irresistibile processo di innovazione che fagocita sempre più dati[34]; o semplicemente per la sua scarsa propensione ad agire, dovuta alla mancata comprensione circa l'immissione delle informazioni in Rete, in forza del già ricordato *privacy paradox*. Così, al fine di riempire di contenuto il diritto alla protezione dei dati personali, la disciplina europea prescrive che il titolare del trattamento sia tenuto a certi obblighi di informazione e ad adottare precise misure tecniche ed organizzative per la tutela degli interessati[35]: la (libera) circolazione delle informazioni riferibili ad una persona fisica è garantita in quanto il trattamento di dati personali sia rivolto a finalità considerate legittime e soprattutto accompagnato da *modalità* che si mostrino, in concreto, rispondenti alla protezione dei diritti della persona[36].

L'altra considerazione cui si accennava ha essenzialmente carattere sistematico. In riferimento alla *data protection by design*, il ruolo del diritto sembra essere quello di orientare, in concreto, la scelta della

---

[34] La debolezza dello strumento della responsabilità aquiliana, per esempio, dinanzi a danni «per definizione seriali e massivi», è sottolineata da C. CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus Civile*, 3, 2020, p. 810.

[35] Il cambio di paradigma del GDPR rispetto alla precedente Direttiva 1995/46/CE è rinvenibile proprio nella gestione del rischio del trattamento dei dati personali, il quale impone l'adozione di una serie di obblighi in capo ai soggetti attivi del trattamento. In questa prospettiva, A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, p. 144 ss. Nell'estendere l'istituto degli "obblighi di protezione" alle misure tecniche ed organizzative cui è tenuto ad adottare il titolare (ed il responsabile) del trattamento, l'impostazione seguita da F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 775 ss., spec. p. 787. Per lo sforzo di combinare ordinamento interno e legislazione comunitaria, riconducendoli a razionalità, si rinvia a A. GENTILI, *Il diritto come discorso*, in *Trattato di diritto privato*, diretto da G. Iudica e P. Zatti, Milano, 2013, p. 227 ss.

[36] Sul punto, cfr. F. G. VITERBO, *The 'User-Centric' and 'Tailor-Made' Approach of the GDPR Through the Principles It Lays down*, in *The Italian Law Journal*, 5(2), 2019, p. 637, secondo il quale «[t]*he problem is establishing whether and how personal data may be processed in each specific concrete online or offline context. That is to say, whether and how the data subject's fundamental rights may be preserved*».

tecnologia più rispondente all'attuazione delle norme che regolano la protezione dei dati personali[37]. Compito del giurista, in particolare, è quello di fornire chiare indicazioni per l'implementazione, pratica ed effettiva, della disciplina applicabile alla protezione dei dati a tutti coloro che si trovano non solo a dover ideare, programmare o sviluppare sistemi informatici, ma anche a *scegliere* quali tra le più diverse tecnologie preposte al trattamento utilizzare[38].

La regola giuridica deve essere, pertanto, letta di concerto alla tecnica, allo scopo di darne effettività[39]. Si può parlare quindi di un *technological enforcement* della protezione dei dati personali, in modo da garantire non solo il corretto funzionamento dei mercati digitali, ma anche e soprattutto la tutela della persona dell'utente[40], alla stregua di quanto è stato definito un vero e proprio "*New Deal*" per il diritto dei consumatori[41].

---

[37] Cfr. B.J. KOOPS – R. LEENES, *Privacy Regulation Cannot Be Hardcoded. A critical comment on the 'privacy by design' provision in data protection law*, in *Int. Rev. Law, Computers & Technology*, 2014(28), p. 168, ove si afferma che la *privacy by design* «*should not be read as a procedural requirement to embed data protection rules as much as possible in system design, but instead as a substantive requirement calling upon data controllers to consistently keep privacy at the front of their minds when defining system requirements*». Ancora, S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, relazione introduttiva al Convegno intitolato "*Internet e privacy - Quali regole?*", Roma, 8 maggio 1998, reperibile *online* all'indirizzo *https://www.privacy.it/archivio/garanterelrod.html*: «Le *privacy enhancing technologies* richiedono questo tipo di riflessione; il riferimento alle norme giuridiche richiede altrettanta riflessione critica. Che tipo di norme giuridiche? Norme giuridiche di tipo stringente o norme giuridiche elastiche, capaci di autoadattarsi alle situazioni che cambiano? Questa è una domanda alla quale dobbiamo rispondere».

[38] Cfr. *considerando* § 78: «(…) In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati».

[39] In una siffatta impostazione, dove l'efficacia giuridica è determinata da regole tecniche non tradotte in regole di fonte legislativa o contrattuale, C. PERLINGIERI, *Profili civilistici dei* social networks, Napoli, 2014, p. 20, nonché P. FEMIA, *Una finestra sul cortile. Internet e il diritto all'esperienza metastrutturale*, in C. PERLINGIERI, L. RUGGERI, *Internet e Diritto civile*, Napoli, 2015, p. 38.

[40] Sulla duplicità di propositi che animano la disciplina europea dei dati personali, N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in Id. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano-Padova, 2019, p. 35 ss.

[41] COMM. EU, *Un "New Deal" per i consumatori*, 11.4.2018, COM(2018) 183 final, p. 4, ove si legge: «Il "*New Deal per i consumatori*" prende le mosse dal quadro esistente della

2.3. Il problema degli strumenti della conoscenza

Non c'è da stupirsi oggi della compiuta perdita di controllo sul flusso di dati personali da parte dell'individuo, da tempo ormai fatta palese[42]. Passando in rassegna le varie "versioni" del *Web*[43], oggi si parla di "vita iper-connessa" – un cambiamento che reca con sé alcuni neologismi, quali il termine *onlife*, che ben esprime la non più netta cesura fra reale e virtuale[44] – la quale si esplica non soltanto nei mercati digitali, ma anche nei rapporti con le pubbliche amministrazioni e, in generale, fra gli stessi consociati (paradigmatico è il caso dei *social network*). Un "ecosistema", questo, dove le attività quotidiane su scala globale ruotano attorno all'utilizzo di dati e le operazioni sono effettuate utilizzando tecnologie *hardware* e soprattutto *software* sempre più sofisticate e, per ampi tratti, riconducibili alle applicazioni dell'Intelligenza Artificiale[45].

Posto che la circolazione di (nuovi) dati personali è incessante e proviene dall'intera comunità digitale – come la pandemia da Covid-19 ha di recente mostrato – altrettanto proporzionalmente decresce però la consapevolezza che ciascuno ha in relazione al trattamento di dati personali. Problemi questi acuiti dall'utilizzo massiccio di assistenti vocali, *wearables*, dall'*Internet of Things*, ove l'utente è tendenzialmente ignaro circa la raccolta di dati personali, per l'assenza o a causa

politica dei consumatori e compie un passo in avanti proponendo norme moderne e adeguate ai mutevoli mercati e prassi commerciali di oggi, strumenti giuridici più efficaci a livello pubblico e privato e migliori possibilità di ricorso». Nella prospettiva tecnologica qui approcciata, v. altresì lo studio intitolato *New aspects and challenges in consumer protection. Digital services and artificial intelligence*, commissionato dallo *European Parliament's committee on the Internal Market and Consumer Protection*, reperibile *online* all'indirizzo https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648790/IPOL_STU(2020)648790_EN.pdf, spec. p. 26 s.

[42] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 82 ss.

[43] K. C. A. Khanzode, R. D. Sarode, *Evolution of the World Wide Web: from Web 1.0 to 6.0*, in *Int. Journal of Digital Library Services,* 6(2), 2016, p. 1 ss.

[44] Interessante ricordare il neologismo "*onlife*", utilizzato da Luciano Floridi, per indicare l'assenza di confini tra la vita *online* e *offline* e, quindi l'assenza di distinzione, dalla prospettiva dell'utente, tra virtuale e reale. V. L. Floridi (ed. by), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Cham, 2015.

[45] Per una panoramica, U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

delle ridotte dimensioni dell'interfaccia grafica del servizio che gli viene reso.

Andando a fondo sul punto, il tema non è tanto legato alla mancanza di trasparenza circa le finalità o i propositi delle operazioni compiute con i dati personali; il problema sembra rinvenirsi piuttosto nella rappresentazione, in concreto, di quali dati personali vengono raccolti, conservati, diffusi, e così via: questi processi – quand'anche fossero comprensibili – rimangono per lo più inaccessibili, nella pratica, per l'interessato, alimentando il *privacy paradox*[46].

Facendo un esempio: coloro che utilizzano intensivamente lo *smartphone* non sono in grado di visualizzare, sia pur in maniera approssimativa, quanti dati sono stati raccolti, nel tempo, effettuando acquisti *online*, utilizzando piattaforme di *car sharing* o *food delivery*, e così via. Ciò si traduce, al di là della mancata percezione delle insidie circa i dati messi in circolo, molto spesso in subdole profilazioni[47], fino a sfociare in limitazioni ovvero discriminazioni, tanto da potersi affermare un nuovo tipo di capitalismo, detto "della sorveglianza"[48].

Tutto ciò è il derivato di un modello di tutela oltremodo inefficiente.

Anzitutto, vi è il diffuso approccio "*notice and consent*", consistente nell'approvazione, da parte dell'interessato, di lunghe, spesso vaghe o, all'opposto, particolarmente dettagliate "informative sul trattamento" – scritte, peraltro, in un linguaggio poco intellegibile ai più[49]: nonostante l'obbligo di fornire all'interessato le informazioni circa il trattamento dei dati personali, l'utente si trova fisiologicamente a

---

[46] Il rapporto tra informazione e trasparenza, dopotutto, è di mezzo a fine, così R. SENIGAGLIA, *Accesso alle informazioni e trasparenza. Profili della conoscenza nel diritto dei contratti*, Padova, 2007, p. 113.

[47] Sui rapporti tra profilazione e il fenomeno della "*filter bubble*", frutto di un uso automatizzato dei dati attraverso algoritmi che crea un effetto di isolamento, in quanto il soggetto è chiuso nel suo profilo, M. BIANCA, *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws – Rivista di diritto dei media*, 2019, 2, p. 1 ss.

[48] Celebre è il volume di S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (trad. it.), Roma, 2019.

[49] H. NISSENBAUM, *A Contextual Approach to Privacy Online*, in *Daedalus*, 140(4), 2011, p. 32 ss.; A. MANTELERO, *The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics*, in *Computer Law and Security Rev.*, 30, 2014, p. 643 ss.; L. GATT, R. MONTANARI, I.A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, p. 339 ss. Più di recente, IDD., *Privacy and Consent. A Legal and UX&HMI Approach*, Napoli, 2021.

dover accettare i termini di servizio pure con riguardo all'utilizzo dei dati, sulla base della condizione (implicita) "*take it or leave it*".

Ancora, poco importa che il GDPR abbia (ri-)affermato una serie di diritti dell'interessato, quali l'accesso ai dati personali, la revoca del consenso, la cancellazione, ecc., se poi l'assolvimento delle richieste presentate da parte del titolare del trattamento rimane ancora lento e macchinoso: non sempre l'interessato si convince ad agire, dal momento che, per la rapidità in cui si muove la realtà virtuale, anche solo spedire una *e-mail* sembra (paradossalmente) essere troppo dispendioso.

Analoghe considerazioni valgono nell'ipotesi di *data breach* [50]: quando la violazione dei dati personali presenta un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve informare l'interessato della natura della violazione, descrivendo «ove possibile (…) le categorie e il numero approssimativo di registrazioni dei dati personali in questione» (art. 33, par. 3, lett. *a*, GDPR). Difficilmente però l'utente è in grado di capire la serietà e la gravità della violazione, se non altro perché non risulta pienamente consapevole della quantità e della qualità di dati personali precedentemente collezionati.

La sfida che qui si delinea – evidenziata anche nella Strategia Europea per i dati[51] – interroga l'ordinamento giuridico sul *come* coinvolgere gli interessati all'interno delle operazioni costituenti trattamento di dati personali, al fine rendere effettivo l'esercizio dei diritti loro riconosciuti[52]. Un compito che sembra essere stato lasciato dal legislatore eurounitario agli stessi titolari del trattamento, mediante un approccio valutativo *ex ante* e basato sul rischio di pregiudizio concreto che l'uso dei dati personali possa determinare in capo ai diritti e alle libertà fondamentali della persona. Ne discende, infatti, l'obbligo per chi utilizza i dati personali di mettere in atto (ed essere in grado di dimostrare l'adozione di) misure organizzative ma soprattutto

[50] Art. 4, par. 1, n. 12, GDPR: «la 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».

[51] COMM. EU, *Una strategia europea per i dati*, cit., p. 23: «È opportuno sostenere ulteriormente le persone nell'esercizio dei loro diritti per quanto riguarda l'utilizzo dei dati che generano, dando loro la possibilità di controllare i propri dati attraverso strumenti e mezzi per poter decidere di volta in volta in dettaglio ciò che può essere fatto con essi».

[52] Quanto all'attuazione del principio di effettività e, alle sue applicazioni concrete, di recente, G. VETTORI, *Effettività fra legge e diritto*, Milano, 2020, p. 63 ss.

tecniche che siano adeguate allo scopo rappresentato e in funzione dei presunti rischi, aventi probabilità e gravità diverse a seconda del trattamento da effettuarsi (art. 24 GDPR)[53].

Individuando un *continuum* sotto il profilo gestionale[54], l'espressa enunciazione del principio della *data protection by design* (art. 25 GDPR) richiama proprio il dovere per il titolare di predisporre misure tecniche e organizzative che siano *adeguate* al trattamento dei dati personali. Ciò non è privo di conseguenze sotto il profilo giuridico, finendo per legittimare la costruzione "fattuale" (*recte* para-normativa) delle regole concernenti i rapporti tra soggetti nell'ambito del trattamento dei dati personali[55]: ancorché i controlli esterni, si avrà modo di vedere, non vengano comunque meno, la legislazione sembra qui arrestarsi, demandando alle forme dell'autoregolamentazione privata, in quanto più vicina agli interessi da disciplinare, il compito di stabilire il complessivo assetto di dettaglio[56].

Operando un mutamento di prospettiva, la questione della trasparenza del trattamento, in particolare, va affrontata allora non tanto sul piano dell'*an*, posto che ricevere certe informazioni è atto dovuto, quanto sul terreno del *quomodo*, cioè con riguardo alle modalità attraverso cui l'interessato può ricevere una rappresentazione chiara e trasparente delle operazioni eseguite con i dati personali. Del resto, quello che ad oggi manca non è tanto l'ideazione, quanto l'implementazione, pratica ed effettiva, di infrastrutture, processi e soluzioni informatiche, quali le *Privacy Enhancing Technologies*, che permettano all'interessato di acquisire, con semplicità e immediatezza, e in

---

[53] Ancora, *considerando* § 74: «È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche».

[54] Cfr. S. CALZOLAIO, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *federalismi.it*, 20 dicembre 2017, p. 14.

[55] In questo senso, F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 801, p. 817, ove si richiama la tesi elaborata da M. MAGGIOLO, *Il contratto predisposto*, Padova, 1996, p. 196 ss., secondo il quale con riguardo ai rapporti giuridici (anche diversi da quelli contrattuali) può aversi un allestimento di un assetto rilevante nella sua materialità, che diviene oggetto di un potere di gestione pur sempre riconducibile all'autonomia privata.

[56] Così P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 213.

sicurezza, una migliore comprensione circa la raccolta, l'uso e la circolazione dei dati personali nell'ambito dei servizi della società dell'informazione.

2.4. L'inclusione dell'interessato nella gestione dei dati personali: i *Personal Information Management Systems*

La soluzione proposta con le specifiche *PETs* volte a rafforzare la trasparenza del trattamento – denominate, per questi motivi, *Transparency Enhancing Tools*[57] – è senza dubbio di segno opposto rispetto alle derive espansionistiche della «società della sorveglianza»[58].

L'interessato viene qui coinvolto, in prima persona, nella gestione dei dati, in modo tale che sia accresciuta la sua consapevolezza del trattamento, almeno nell'accezione "minima" di controllo (ad esempio, con chi condivido i dati, per quanto tempo, per quali finalità, etc.). Tuttavia, non basta soltanto fornire la visualizzazione in tempo reale dei dati personali raccolti dal titolare del trattamento, bensì tali meccanismi tecnici devono agevolare altresì il concreto e pratico esercizio dei diritti riconosciuti all'interessato, come la cancellazione, la rettifica, la revoca del consenso, la portabilità dei dati personali, e così via.

Nella prospettiva delineata, particolare rilievo assumono i c.d. *Personal Information Management System* – che forse sarebbe più opportuno rinominare, alla luce del GDPR, *Data Protection Management Tools*[59]. Si tratta di una "architettura" di trattamento dei dati personali consistente per lo più in sistemi *software* mediante i quali l'utente interviene direttamente nel processo di raccolta, conservazione e diffusione dei dati, venendosi a creare, programmaticamente, una nuova realtà «in

---

[57] D. Spagnuelo, A. Ferreira, G. Lenzini, *Transparency Enhancing Tools and the GDPR: Do They Match?*, in P. Mori, S. Furnell, O. Camp (edited by), *Information Systems Security and Privacy*, Cham, 2020, p 162 ss.; C. Zimmermann, A *Categorization of Transparency-Enhancing Technologies*, in *arXiv*, 2015, https://arxiv.org/ftp/arxiv/papers/1507/1507.04914.pdf.

[58] D. Lyon, Z. Bauman, *Sesto potere. La sorveglianza nella modernità liquida*, Roma-Bari, 2014.

[59] Per una prima analisi, EDPS, *Opinion 9/2016 on Personal Information Management Systems. Towards more user empowerment in managing and processing personal data*, 20.10.2016, reperibile *online* all'indirizzo https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf, nonché, da ultimo, EDPS, *Opinion 3/2020 on the European startegy for data*, 16.6.2020, reperibile *online* all'indirizzo https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf.

cui le persone gestiscono e controllano la propria identità *online*»[60]. Ciò è reso possibile attraverso il coinvolgimento *diretto* degli interessati, i quali possono interagire con i propri dati, per esempio, scegliendo i destinatari con cui condividerli ovvero le categorie di informazioni oggetto di trattamento ulteriore per finalità diverse da quelle iniziali, o ancora eliminando particolari contenuti informativi, considerati non più rilevanti. Sicché l'obiettivo di garantire una più *accessibile* gestione dei dati personali – dal ricevere le informazioni in merito al trattamento in essere sino all'effettivo esercizio del diritto alla cancellazione – trova una risposta attraverso l'implementazione di semplici e immediate soluzioni interattive di tipo "*point and click*"[61].

Potenzialmente, un sistema del genere permette di riequilibrare, per un certo verso, l'asimmetria (informativa) per la quale l'interessato manca, di fatto, degli strumenti tecnici per controllare adeguatamente il trattamento di dati personali. Così, l'approccio statico, ancora largamente diffuso tra i titolari del trattamento, dovrebbe dirigersi verso un'inclusione *dinamica* dell'interessato all'interno della gestione dei dati personali. In questo modo, sembra mutare anche il ruolo assunto della persona fisica, da soggetto passivo, inerte, a parte attiva dell'economia digitale, rafforzandosi l'autodeterminazione informativa del singolo.

È bene notare come una maggiore trasparenza non deve assolutamente condurre all'esito opposto di *information overload*, nell'ipotesi di troppe informazioni specifiche che non beneficiano affatto l'utente (e neanche il fornitore del servizio digitale): i criteri da seguire, e che limitano la discrezionalità di chi adotta, in pratica, le diverse tecnologie, sono quelli della necessità, della proporzionalità e della

---

[60] Testualmente «*[t]he PIMS concept offers a new approach by which individuals are the holders of their own personal information*»: così EDPS, Opinion 9/2016, cit., p. 5.

[61] H. JANSSEN, J. COBBE, J. SINGH, *Personal information management systems: a user-centric privacy utopia?*, in *Internet Policy Review*, 9(4), 2020, p. 1 ss.; A. CRABTREE, T. LODGE, J. COLLEY, C. GREENHALGH, K. GLOVER, H. HADDADI, Y. AMAR, R. MORTIER, Q. LI, J. MOORE, L. WANG, P. YADAV, J. ZHAO, A. BROWN, L. URQUHART, D. MCAULEY, *Building accountability into the Internet of Things: the IoT Databox model*, in *Journal of Reliable Intelligent Environments*, 4(1), 2018, p. 39 ss.; A. POIKOLA, K. KUIKKANIEMI, H. HONKO, *MyData – A Nordic Model for human-centered personal data management and processing*, 2015, [white paper], reperibile *online* all'indirizzo https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf.

ragionevolezza di ciò che dev'essere visualizzato[62]. In questo senso, è opportuno sia attribuita una attenzione particolare alle preferenze di coloro che usufruiscono dei diversi servizi della società dell'informazione[63]: l'accettabilità e l'usabilità degli utenti sono elementi fondamentali dei quali tenere conto nelle scelte delle misure tecniche da adottare in concreto[64].

Ancora una volta, sono facilmente comprensibili i limiti che incontra la regolazione, se intesa soltanto come normazione pubblica eteronoma, in ragione della rapida obsolescenza delle regole di dettaglio dinanzi all'innovazione tecnologica[65]; o ciò che è lo stesso, pare impossibile prescindere, in questi casi, dal potere normativo dei soggetti privati nella protezione dei dati personali. Più precisamente, al fine di rafforzare la tutela della persona nell'ambiente digitale, non può non considerarsi il ruolo assunto dai titolari del trattamento, ai quali è affidato l'obbligo di garantire che i mezzi mediante i quali si realizza il trattamento di dati personali siano rispondenti ai principi generali applicabili alla protezione dei dati personali; ciò nell'ottica di quella *accountability* sopra ricordata, per la quale si rende necessaria l'adozione di misure tecniche e organizzative – sistemi, processi, protocolli, tecnologie[66] – *adeguate* al tipo di trattamento da espletarsi, tenuto conto «dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i

---

[62] Per una completa analisi del principio di ragionevolezza e di proporzionalità nel diritto civile, G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015.

[63] A. Mantelero, Digital privacy*: tecnologie "conformate" e regole giuridiche*, in F. Bergadano, A. Mantelero, G. Ruffo, G. Sartor (a cura di), Privacy *digitale. Giuristi e informatici a confronto*, Torino, 2005, p. 19 ss.

[64] Seppur in ambito parzialmente diverso, pare opportuno richiamare quanto affermato da Art. 29 WP, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, 6 febbraio 2018, reperibili *online* all'indirizzo https://ec.europa.eu/newsroom/article29/items/612053: al titolare del trattamento è imposto di fornire informazioni sulla logica utilizzata nei processi decisionali automatizzati, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati. Le informazioni fornite dovrebbero comunque essere sufficientemente complete affinché l'interessato possa comprendere i motivi posti alla base della decisione.

[65] D. Di Sabato, *Diritto e* new economy, Napoli, 2020, p. 27.

[66] Cfr. F. Romeo, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., p. 1261: «Il diritto deve essere costruito dentro alla tecnica stessa, per evitare l'attuale stato di ineffettività di tante statuizioni ed inapplicabilità di tante interpretazioni».

diritti e le libertà delle persone fisiche costituiti dal trattamento» (art. 25, par. 1, GDPR), coniugando di quest'ultimo l'aspetto strutturale con la funzione che la protezione dei dati personali intende garantire nei confronti dell'interessato[67].

2.5. Il principio di *data protection by design* come criterio di selezione

Si è visto, discorrendo di *data protection by design*, che l'elemento strutturale relativo alla predisposizione delle tecnologie del trattamento si salda con l'aspetto funzionale cui esse sono rivolte, allo scopo di garantire, per un verso, la legittimità del trattamento, la trasparenza, la minimizzazione dei dati, etc., nonché la tutela dell'interessato, rendendo finanche possibile l'esercizio pratico dei diritti a quest'ultimo riconosciuti dal GDPR[68].

Non è corretto però ritenere che le *Privacy Enhancing Technologies* debbano intervenire soltanto *a posteriori*, per rinforzare, alla stregua di particolari misure di sicurezza, i principi e le regole relative al trattamento su sistemi non pensati *ex ante* per integrare nella loro struttura la protezione dei dati personali[69]. Diversamente, la strategia portata avanti con le *PETs* richiede la scelta ponderata di tecnologie adeguate alla normativa sulla protezione dei dati personali già in fase di programmazione delle operazioni da svolgersi, secondo un *prius* logico

[67] Per R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 83, l'operare dell'art. 25 GDPR si esplica in un quadro variabile, in relazione sia alla gravosità dell'impegno, sia in base ai costi da sostenere.

[68] Ciò trova conferma in una lettura teleologicamente orientata dell'art. 25, par. 1, GDPR, laddove «(…) il titolare del trattamento mette in atto misure tecniche e organizzative adeguate (…) volte ad attuare in modo efficace i principi di protezione dei dati (…) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

[69] Cfr. S. CALZOLAIO, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, cit., p. 16. Come osserva R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 103, le *PETs* sono frutto di un approccio "ingegneristico" alla tecnologia volto a ricavarne dispostivi più "virtuosi" di tutela dei dati personali, mentre le "misure" di cui all'art. 25 GDPR riflettono una concezione più ampia, la quale unisce l'elemento tecnologico con le regole giuridiche che condizionano il trattamento dei dati personali.

rispetto al successivo trattamento[70]. Infatti, l'adozione di talune soluzioni, tra quelle messe a disposizione del titolare, non incide soltanto sul momento ideativo del trattamento, in modo statico[71]; al contrario, le misure predisposte sono pensate, in quanto congegnate già in fase di programmazione delle attività come indirizzate alla protezione dei dati personali, per coprire l'intero "ciclo vitale" del trattamento, e come tali richiedono un costante aggiornamento, in maniera dinamica[72].

Ora, è pacifico che il GDPR abbia recepito il principio di *digital neutrality*, secondo il quale la norma giuridica non consiglia l'adozione di una o l'altra tecnologia[73]. Eppure, la scelta di una certa tecnologia è influenzata dalla regola giuridica da applicare, la quale, sia pur nella complessità dell'ordinamento, seleziona gli interessi meritevoli di protezione nel caso concreto e li colloca entro una scala assiologica[74]; così accade anche per le norme poste a presidio del trattamento dei dati personali, le quali, nel contesto applicativo, pure quando si relazionano con gli apparati tecnologici, rispondono comunque agli scopi di tutela tracciati dal diritto[75].

---

[70] Cfr. EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, v. 2.0, 20.10.2020, reperibili *online* all'indirizzo https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, p. 10, ove si afferma che «(…) *from a cost-benefit perspective, it is also in controllers' interest to take DPbDD into account sooner rather than later, as it could be challenging and costly to make later changes to plansthat have already been made and processing operations that have already been designed*».

[71] Se non per i c.d. *system level requirements* come osservano B.J. KOOPS, R. LEENES, *Privacy Regulation Cannot Be Hardcoded*, cit., p. 162.

[72] F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 790.

[73] Cfr. *considerando* § 15: «Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate». Sul punto, D. FARACE, Privacy by design *e* privacy by default, in E. TOSI (a cura di), Privacy *digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 499.

[74] Lo sottolinea C. PERLINGIERI, *La tutela dei minori di età nei* social networks, in *Rass. dir. civ.*, 2016, p. 1331, in quanto le regole tecniche, se sono di per sé neutrali, perdono il carattere della neutralità quando divengono struttura logica di interconnessioni soggettive e devono essere valutate sotto il profilo della legittimità.

[75] Così anche S. RODOTÀ, *Libertà, opportunità, democrazia, informazione*, cit., secondo il quale «[n]on siamo di fronte a tecnologie neutre, neutrali; siamo di fronte a tecnologie in cui si manifesta al massimo grado la forza di modello sociale della rete e quindi esigono una seria discussione sul quadro istituzionale, all'interno del quale noi possiamo muoverci e dobbiamo muoverci». Del resto, il GDPR intende porsi come uno *standard* globale di tutela dei dati personali, come affermato da G. BUTTARELLI, *The EU*

Del resto, come il diritto può vietare il ricorso a certi strumenti tecnologici, viceversa, la tecnica può determinare l'inefficacia della norma giuridica[76]: la questione allora non è tanto quali regole o quali tecniche adottare, in astratto; il nodo cruciale sta nell'individuare una connessione *teleologica* tra le finalità perseguite (e gli interessi coinvolti) nel trattamento di dati personali e i mezzi con i quali esso si esplica, in concreto, avuto riguardo alla *scelta* della tecnologia da adottare, alla luce della tutela della persona. In questo senso, la prerogativa di stabilire ciò che è lecito o meno nell'uso di una certa tecnologia spetta al diritto, il quale determina così una funzionalizzazione degli interessi (*recte* conformazione) anche con riferimento alla tecnica.

Facendo un esempio: la quantità e la qualità di informazioni rese all'interessato in merito al trattamento possono essere rappresentate in varie forme, ma alcune modalità – e le conseguenti misure da adottare – rimangono più adeguate di altre per accrescere la trasparenza e l'accesso alle informazioni da parte dell'utente, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

a) Una efficace rappresentazione sia dei dati personali, sia del trattamento, trascorre necessariamente per l'interfaccia-utente e quindi per la grafica[77]. Così, una semplice "lista" dei dati raccolti si mostrerebbe come una soluzione inefficiente; sembra preferibile, invece, l'adozione di un sistema dove i dati personali siano raggruppati per

GDPR as a clarion call for a new global digital gold standard, in *Int. Data Privacy Law*, 2016, p. 77.

[76] O potenzialmente essere migliore della norma giuridica nel plasmare i comportamenti dei consociati. Per il dibattito sviluppatosi circa *lex informatica*, L. LESSIG, *Code and Other Laws of Cyberspace*, New York, 1999, per il quale una certa architettura della Rete (il *code*), dal punto di vista eminentemente tecnico, è in grado di condizionare talune (o altre) condotte degli utenti, permettendole o inibendole in via automatica; su una posizione diversa, S. RODOTÀ, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 2002. Sul tema specifico indagato anche J. D. REIDENBERG, Lex informatica*: The Formulation of Information Privacy Rules Through Technology*, in *Texas Law Review*, 76(3), 1998, p. 553 ss.

[77] Per il maggiore adeguamento ai principi della *user experience* delle interfacce *web* in relazione alla *data protection*, vedi P. COSTA, User experience design *e dati personali: come (ri)progettare la privacy*, in B. PASA (a cura di), *Design e innovazione digitale. Dialogo interdisciplinare per un ripensamento delle tutele*, Napoli, 2021, p. 142 ss.; ancora, H. HAAPIO, M. HAGAN, M. PALMIRANI, A. ROSSI, *Legal Design Patterns for Privacy*, in E. SCHWEIGHOFER ET AL. (edited by), *Data Protection / LegalTech*, *Proceedings of the 21th International Legal Informatics Symposium 2018*, Berna, 2018, pp. 445–450.

diverse categorie semantiche, usando vari colori, diagrammi, o ancora icone standardizzate, elementi percentuali o intervalli di tempo.

b) Assai utile, per l'implementazione effettiva della trasparenza, è la costruzione di un sistema multilivello, dove le informazioni più rilevanti siano poste visivamente in primo piano. Ciò dovrebbe essere reso possibile, in particolare, per coloro che non abbiano una sufficiente educazione quanto alle insidie del mondo digitale, in particolare minori e anziani[78]. Inoltre, molti utenti potrebbero non ritenersi soddisfatti del contenuto minimo informativo così presentato dal *digital provider*; pertanto, è più spendibile una tecnologia che preveda l'integrazione di diverse finestre (o *pop-up*) man mano contenenti maggiori informazioni, dove quelle essenziali vengono indicate con "enfasi" maggiore.

c) Un sistema di notifiche, ancora, permette di definire in maniera chiara e semplice le operazioni successive alla raccolta, con particolare riferimento alla comunicazione e diffusione di dati personali. Inoltre, un *alert* potrebbe avvisare l'interessato nell'ipotesi di un *data breach*, descrivendo meglio i dati oggetto di divulgazione non autorizzata, come anche, in generale, rendere edotto l'utente circa le minacce rilevate, specie in caso di sovraesposizione a causa di una eccessiva raccolta di dati personali e, di conseguenza, suggerire l'azione successiva da intraprendere.

d) Un ulteriore aspetto da valutare è quello di prevedere una sorta di pannello intuitivo di controllo che costituisca un'interfaccia altamente personalizzabile e attrattiva, mediante la quale comunicare in tempo reale con il titolare del trattamento (ad esempio, una particolare *dashboard* dedicata, quale *feature* specifica della *app*), come se fosse una sorta di *customer service* dedicato ai dati personali. Tutto ciò renderebbe altresì molto più semplice esercitare concretamente i diritti dell'interessato.

In buona sostanza, la *data protection by design* richiede che i requisiti legali relativi al trattamento di dati personali non siano tradotti in termini algoritmici, come si suole affermare[79], bensì implementati nella *scelta* di misure tecniche e operative adeguate, ragionevoli e proporzionate alla situazione specifica, garantendo, per questa via,

---

[78] In argomento, G. Malgieri, J. Niklas, *Vulnerable data subjects*, in *Computer Law and Security Review*, 37, 2020, p. 1 ss.

[79] Con una critica efficace, v. B.J. Koops, R. Leenes, *Privacy Regulation Cannot Be Hardcoded*, cit., p. 166.

l'effettività della disciplina che governa la protezione dei dati personali. In ogni caso, si tratta di criteri dinamici, flessibili ed empirici, il cui contenuto è da valutarsi nella situazione specifica, o di una serie omogenea di casi, a seconda degli interessi di volta in volta richiamati. Vieppiù che tali criteri muovono dall'essere metro di misura dell'adozione di tecnologia a «tecnica argomentativa»[80] per attuare il principio di *accountability* e, in ultimo, essere parametro di giudizio per la congruità delle misure adottate per la tutela dei dati personali.

D'altro canto, «una buona regolamentazione, se pur essenziale, non è sufficiente»[81]; semmai la norma giuridica deve orientare la realizzazione degli algoritmi, coordinandosi, da un lato, con le altre scienze e, dall'altro, guidando gli operatori pratici nelle decisioni relative all'implementazione dei principi e delle regole attraverso le tecnologie; verificando, in seguito, se l'effettività delle tutele sia raggiunta, soprattutto in ragione delle alternative tecniche, della complessità e dei repentini mutamenti dell'era digitale[82].

In questa prospettiva, i codici di condotta[83], i meccanismi di certificazione[84], ma anche i *privacy design patterns*[85], i quali rappresentano varie combinazioni prefissate di misure tecniche e organizzative di possibile adozione, costituiscono tutti strumenti fondamentali attraverso i quali definire l'architettura del trattamento, specialmente nella fase di predisposizione dei sistemi informatici, nonché di una loro successiva modifica o revisione. A ciò si aggiungono, naturalmente, le previsioni fornite dalle autorità di controllo, nazionali ed europee, in funzione propulsiva, autorizzativa o partecipativa con riguardo a siffatte nuove espressioni della giuridicità – specie per i menzionati codici di

---

[80] Così R. D'ORAZIO, *Protezione dei* dati by default *e* by design, cit., p. 95 ss.

[81] EDPS, *Opinion 9/2016*, cit., p. 14 («*Good regulation, while crucial, is not sufficient in itself*»), ove si sottolinea come il contributo offerto dalla tecnologia appare essenziale nell'affermazione dei *PIMS*.

[82] Effettività più volte ricordata anche dall'EDPB, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, cit. (per ben 51 volte!).

[83] D. POLETTI, M. C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI, Privacy *digitale*, cit., p. 369 ss.

[84] Ad es., si potrebbe pensare allo *standard* già esistente ISO/IEC 27701 sui *Privacy Information Management System* (PIMS), inteso come una estensione della ISO/IEC 27001 e ISO/IEC 27002 su *privacy management*.

[85] In argomento, J. LENHARD, L. FRITSCH, S. HEROLD, *A Literature Study on Privacy Patterns Research*, 2017, 43rd *Euromicro Conference on Software Engineering and Advanced Applications*, reperibile *online* all'indirizzo https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8051348, pp. 194 ss.

condotta e meccanismi di certificazione[86] –, ben diverse dalla regola intesa in senso formale: il che si traduce in una strategia di normazione integrata, che si delinea, appunto, come un'autonomia (privata) "controllata"[87].

Tutto ciò rende, in definitiva, l'algoritmo e soprattutto la tecnologia stessa "testabile" e "contestabile"[88], non solo da parte dell'utente, ma anche dagli altri soggetti che partecipano attivamente nei mercati digitali, come i titolari (e i responsabili) del trattamento, le autorità di controllo e, non da ultimo, i legislatori[89].

2.6. L'esempio dei *Personal Data Stores*: un modello vincente?

Dotare gli utenti dei servizi digitali di strumenti tecnologici per meglio interfacciarsi con il trattamento dei dati personali è senz'altro funzionale ad accrescere la loro consapevolezza in merito all'utilizzo che viene fatto delle informazioni ad essi riconducibili, come anche a rafforzare la loro autonomia nell'alveo del capitalismo dell'informazione.

In questo frangente, si inserisce una particolare tipologia di *PIMS*, noto come *Personal Data Store*[90]. In sostanza, si tratta di un'alternativa al classico sistema di memorizzazione dei dati personali all'interno dei *server* centralizzati (*silos*) sotto il controllo diretto dei *digital providers*[91]:

---

[86] Per fare un esempio: l'art. 57, GDPR, individuando i compiti delle autorità di controllo, indica espressamente quello di incoraggiare l'elaborazione di codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma del procedimento indicato nell'art. 40 GDPR. Analogo discorso può farsi con i meccanismi di certificazione di cui all'art. 42 GDPR.

[87] Cfr. S. RODOTÀ, *Tecnologie e diritti*, cit., p. 51 ss.; più di recente, P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 110 ss.

[88] M. HILDEBRANDT, *Saved by Design? The Case of Legal Protection by Design*, in *Nanoethics*, 2017, p. 309.

[89] Vedi sul punto P. LAGHI, *Cyberspazio e sussidiarietà*, cit., p. 115, ove si riconosce la maggiore idoneità regolativa dell'autonomia privata organizzata (c.d. *co-regulation*) nel soddisfacimento degli interessi coinvolti, mantenendosi però un ruolo di direzione e di orientamento del potere pubblico che consente di supplire ad essa allorché si dimostri incapace di realizzare un assetto equilibrato.

[90] H. JANSSEN, J. COBBE, C. NORVAL, J. SINGH, *Decentralised Data Processing: Personal Data Stores and the GDPR*, in *Int. Data Privacy Law*, 9, 2020, p. 356 ss. e ivi ampi riferimenti bibliografici.

[91] T. LEHTINIEMI, *Personal Data Spaces: An Interventation in Surveillance Capitalism*, in *Surveillance & Society*, 15(5), p. 631.

il modello proposto è di stampo decentralizzato, dal momento che i dati personali di ciascun utente vengono memorizzati solo in locale sui singoli *device* in possesso dell'individuo, ovvero su un *cloud*, fornito, di solito, da un soggetto terzo; sicché i diversi fornitori di servizi digitali possono solo accedere al *PDS* in maniera selettiva, a seconda delle preferenze accordate dall'utente, caso per caso, o in una serie omogenea di casi, senza la possibilità di "replicare" i dati oppure di svolgere la analisi al di fuori del "luogo virtuale" prescelto[92].

Oltre ad essere in grado di percepire meglio quali dati personali vengono utilizzati da altri soggetti, gli utenti sono messi in condizione di esercitare in maniera più agevole i diritti loro spettanti, come la rettifica e la cancellazione dei dati, il diritto di opposizione o la revoca del consenso al trattamento, o ancora il diritto alla portabilità dei dati, posto che l'esistenza di *standard* compatibili e di formato, con riguardo all'esistenza di un singolo spazio virtuale, rendono più semplice il trasferimento di dati. Anzi, a maggior ragione, i *PDS* possono fungere da vero e proprio collettore di dati relativi a molteplici servizi della società dell'informazione e, per certi versi, ricostruire l'identità personale, sempre più frammentata nella "data-sfera"[93].

È auspicabile, dunque, l'utilizzo dei *PDS*, i quali permettono all'individuo decisioni più consapevoli in merito al trattamento dei dati personali e un controllo effettivo e concreto delle informazioni riguardanti la persona, laddove quest'ultima è davvero posta al centro della scena, mediante un approccio inclusivo e non alienante, nell'incessante processo di "datificazione" della sfera privata. E come un circolo virtuoso, l'adozione di tali strumenti, che senz'altro rinforzano la trasparenza del trattamento, dovrebbe permettere all'interessato di acquisire maggiore fiducia e affidabilità nei servizi offerti nella società dell'informazione, in quanto resi con modalità più accessibili e comprensibili[94].

---

[92] Cfr. EDPS, *Opinion 9/2016*, cit., p. 6. Per un modello opposto a quello del *PDS*, laddove l'intermediario è delegato dall'interessato ad ottenere i dati personali presso i diversi titolari del trattamento, allo scopo di riunirli in un'unica banca dati per "monetizzarne" l'uso, F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO, A. RIZZO, M. TESCARO, *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 93 ss.

[93] Sul significato di tale espressione, V. ZENO-ZENCOVICH, *La "Datasfera". Regole giuridiche per il mondo digitale*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, 99 ss.

[94] In questo senso, v. anche EDPS, *Opinion 9/2016*, cit., p. 8. Si rafforza così il coordinamento tra disciplina posta a presidio della circolazione dei dati personali, la tutela dei consumatori e la concorrenza nel Mercato Unico Digitale.

Quanto appena affermato, letto alla luce del principio della *data protection by design*, implica una rottura del paradigma *company-centric* tuttora diffuso, indirizzando le misure tecniche e organizzative, delle quali si serve il titolare del trattamento, verso un approccio maggiormente *user-oriented*. Così, i *PDS* possono essere visti come strumenti tecnologici che forniscono all'individuo uno "sguardo all'interno" del trattamento, considerando, tra l'altro, come la raccolta dei dati spesso avvenga al primo contatto con l'interessato, mentre difficilmente in seguito si vanno a modificare le scelte accordate. Inoltre, i *PDS* rappresentano una occasione d'intervento nel capitalismo di sorveglianza, andando ad attribuire agli interessati un ruolo operativo nelle dinamiche relative alla circolazione dei dati personali, fronteggiando apertamente i pericoli di un trattamento "oscuro" non tanto per le finalità, ma soprattutto per i mezzi impiegati, specie quando vi sia un uso intensivo di prodotti dell'Intelligenza Artificiale e delle tecniche di *machine learning*.

Nondimeno, la soluzione dei *PDS* solleva alcune questioni sotto l'ambito di applicazione del GDPR[95]. Tra le tante, non è affatto semplice individuare il ruolo (e le relative responsabilità) dei gestori del *PDS*, potendo agire, di fatto, quali titolari del trattamento, responsabili, o ancora come titolari "autonomi" (*recte* "terzi"[96]). Posto che gli utenti non possono essere considerati come "titolari" (del trattamento) quanto alle informazioni ad essi riconducibili, una possibile soluzione potrebbe essere vista nella contitolarità del trattamento, laddove i vari soggetti che operano con i dati personali, accedendo ai *PDS*, regolano preventivamente e attraverso lo strumento contrattuale rispettivi obblighi e responsabilità, sia nei confronti dell'interessato, sia tra di loro[97].

---

[95] Cfr. H. JANSSEN, J. COBBE, C. NORVAL, J. SINGH, *Decentralised Data Processing: Personal Data Stores and the GDPR*, cit.

[96] Art. 4, n. 10, GDPR: «"terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile».

[97] Interessanti sono le indicazioni fornite dall'EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, v. 1.0, 2.9.2020, spec. p. 40 sul concetto di *joint controllership* di cui all'art. 26, GDPR, laddove si richiama la pronuncia CGUE, 5 giugno 2018, causa C-210/6, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein c. Wirtschaftsakademie Schleswig-Holstein GmbH* (pubblicata in *Foro it*., 2018, IV, c. 361, con nota di richiami di R. PARDOLESI e S. BONAVITA), dove i giudici hanno ritenuto l'amministratore di una *fan page* ospitata su *Facebook* e il noto *social network* come

L'esplosione di un mercato di servizi *PDS* è ancora più complicato[98]. L'implementazione pratica di un siffatto modello deve fare i conti con l'idea di *business* ancora basata sul capitalismo predominante dell'impresa, e non sulla persona dell'utente. Ciò è dovuto, principalmente, alla presenza di pochi monopolisti (soprattutto i *Tech Giants*), i quali hanno accresciuto la quantità di utenti (e di dati) in loro possesso, anche grazie agli effetti di rete di accaparramento della clientela, determinando, di fatto, delle forti barriere all'ingresso di nuovi *competitor* nei mercati digitali[99]. L'assenza di vantaggi competitivi per tali categorie di soggetti non può che tradursi in una carenza di interesse quanto alla diffusione di strumenti informatici più incentrati sulla persona.

Ora, se per le attività nelle quali il *core business* non è rappresentato dall'accumulo di dati personali l'adozione dei *PDS* vedrebbe facilmente ridotti i costi di *compliance* e i rischi inerenti a possibili violazioni di sicurezza, mediante l'affidamento della loro gestione a un terzo "fiduciario", cambiare l'attuale assetto della *Big Data economy* appare ancora molto distante, con pochi soggetti che godono ancora di una "rendita da posizione". Qui forse solo la trasparenza potrebbe giocare un ruolo chiave di incentivo: si passerebbe, in tal senso, da un modello di mercato basato sulla *data rentention* ad uno in cui la qualità del servizio offerto costituisce la chiave per assicurarsi un maggior numero di clienti; di conseguenza, gli utenti sarebbero propensi a fornire dati sempre più precisi e aggiornati, in quanto interessati a ricevere servizi costruiti in base alle loro *attuali* preferenze – il che porterebbe, peraltro, ad una migliore profilazione della clientela. Ulteriori stimoli potrebbero rinvenirsi, poi, nella semplificazione delle attività condotte dal

contitolari del trattamento rispetto agli utenti della pagina; più di recente, CGUE, 29 luglio 2019, causa C-40/17, *Fashion Id Gmbh & Co. Verbraucherzentrale Nrw Ev, Facebook Ireland Ltd Landesbeauftragte Fu¨R Datenschutz Und Informationsfreiheit Nordrhein-Westfalen*, in *Dir. inf.*, 2019, p. 1253 ss., con nota di G. GIANNONE CODIGLIONE, *Trattamenti multipli di dati personali e parcellizzazione degli obblighi di condotta*.

[98] Per l'analisi di alcune soluzioni di mercato, I. BOLYCHEVSKY, S. WORTHINGTON, *Are Personal Data Stores about to become the NEXT BIG THING?*, https://medium.com/@shevski/are-personal-data-stores-about-to-become-the-next-big-thing-b767295ed842; T. BERNERS-LEE, *We Need to Change How We Share Our Personal Data Online in the Age of COVID-19*, in *Time*, 15 luglio 2020, reperibile all'indirizzo https://time.com/5867314/we-need-to-change-how-we-share-our-personal-data-online-in-the-age-of-covid-19/.

[99] Sul punto, diffusamente, T. LEHTINIEMI, *Personal Data Spaces*, cit., p. 626 ss.

titolare, nonché, da ultimo, in una migliore immagine guadagnata dall'impresa[100].

2.7. La trasparenza quale presupposto per la scelta "democratica" della tecnologia

La trasparenza costituisce un elemento cruciale dell'intero sistema di scelta della tecnologia nel trattamento di dati personali in funzione della persona, dal momento che funge non solo da connettore delle diverse operazioni in cui esso si esplica, ma garantisce anche, coordinando le finalità e i mezzi del medesimo, l'effettività dei diritti che il GDPR ha riconosciuto all'interessato e, per questa via, rafforza pure la tutela dei diritti e delle libertà fondamentali dell'individuo.

Si è già visto come le tecnologie volte ad implementare il principio della trasparenza nel trattamento dei dati personali possano essere utilizzate per bilanciare l'asimmetria informativa esistente tra i *digital service provider* e i loro fruitori, accrescendo il potere di controllo degli interessati quanto alle informazioni ad essi riconducibili. Infatti, le soluzioni offerte da *PIMS* e *PDS* sembrano fornire una maggiore conoscenza della circolazione dei dati personali nell'ambiente digitale, connettendo la prospettiva *ex ante* (ottenere dal titolare le informazioni obbligatorie circa il trattamento effettuato) con quella *ex post* (relativamente all'esercizio dei diritti riconosciuti all'interessato), non più tenute distinte, ma saldate in un circolo virtuoso fra il titolare e l'interessato.

Sotto un diverso profilo, gli strumenti sopra ricordati potrebbero risolvere alcuni problemi derivanti dall'universo *IoT*, dove il più delle volte risulta difficile rendere le informazioni chiare e comprensibili quanto al trattamento, stante la ridotta dimensione o addirittura l'assenza di un *display* con il quale visualizzare i dati, continuamente collezionati attraverso il servizio digitale; cosicché l'esistenza di un *PDS* dedicato, che consenta di gestire i dati personali dell'interessato, condurrebbe non solo al rafforzamento del ruolo dell'utente, ma anche a

[100] Per un'approfondita analisi di mercato, *Study commisioned to Cambridge Judge Business School* intitolato *Personal Data Stores* [Report], Cambridge University, 2015, reperibile *online* all'indirizzo https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school.

rendere più chiaro l'operato del fornitore del servizio legato all'"oggetto connesso".

Quello che ancora manca per il concreto funzionamento delle *PETs* è l'educazione digitale degli utenti della Rete, senz'altro carente in merito ai rischi e ai pericoli che l'ambiente *online* porta con sé, come dimostrato dal *privacy paradox*[101]. In questo senso, soccorrerebbe, ancora, la *data protection by design*, in funzione "formativa" della persona: se l'architettura del sistema di gestione dei dati personali viene davvero predisposta dal titolare del trattamento in maniera più trasparente e a misura d'utente, tenuto conto dei rischi e del contesto situazionale, non solo il pieno rispetto del GDPR, ma anche il reciproco rapporto tra fornitore di servizio digitale e il cliente non può che uscirne migliorato; il tutto nella prospettiva di una tutela effettiva degli individui, sia pure risultato di una compartecipazione fra regola tecnica e norma giuridica, autoregolamentazione e controllo esterno, mercato e persona.

La *data protection by design* non è, dunque, un concetto rigido o statico, dal momento che al titolare del trattamento si richiede una attenta e continua valutazione non solo dei rischi per i diritti e le libertà fondamentali dell'interessato, ma anche del contesto e soprattutto degli interessi in forza dei quali si compiono le operazioni con i dati personali. Sicché l'effettività della protezione dei dati personali non può essere lasciata alla sola tecnica, men che meno al solo diritto[102]. Al contrario, il *test* di adeguatezza, proporzionalità e ragionevolezza dell'adozione di una certa tecnologia utilizzata nel trattamento deve necessariamente prendere in considerazione, tre le presenti (e future) alternative, la tutela degli interessi giuridicamente meritevoli di

[101] Nel senso che tecnologie di *data control by design* permettono all'utente non solo una gestione modulare dei dati personali con il vantaggio di formare in esso un "migliore" consenso al trattamento, ma anche una maggiore educazione sui rischi e sugli usi cui sono esposte le informazioni che lo riguardano, v. altresì A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019, p. 213, nota 109. In una più ampia prospettiva, M. D'AMBROSIO, *Progresso tecnologico, "responsabilizzazione" dell'impresa ed educazione dell'utente*, Napoli, 2017, p. 112 ss. Nondimeno, pure il settore dell'*eGovernment* potrebbe essere considerato come un settore promettente, specie quello sanitario: COMM. EU, *An emerging offer of "personal information management services". Current state of service offers and challenges*, 2015, reperibile *online* all'indirizzo https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118, p. 13.

[102] F. ROMEO, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, cit., p. 1270, secondo il quale il governo della tecnica presuppone la conoscenza delle sue regole, dal momento che il diritto deve essere in grado di interagire con essa al fine di orientare i risultati verso gli scopi posti dalla norma giuridica.

protezione, nelle specifiche circostanze del caso. In fondo, la norma giuridica non può certo perdere la sua funzione di valutare gli strumenti migliori per tutelare gli interessi protetti.

Posto che la definizione degli algoritmi e delle tecnologie non assicura la medesima partecipazione democratica presente a livello della regolamentazione legislativa, è proprio attraverso il sindacato di legittimità circa l'autonomia della scelta – quand'anche relativa alle misure, in concreto, da adottare – e specialmente degli obblighi gravanti sui titolari del trattamento, sin dal momento di determinare i mezzi dello stesso, che si coniugano la tecnologia in termini democratici e la sua rispondenza ai valori costituzionali riferibili alla persona.

Nell'era digitale, la tutela dell'individuo, per considerarsi davvero effettiva, deve essere perciò supportata dalle medesime tecnologie che rendono possibile il trattamento di dati personali per i fornitori di servizi nella società dell'informazione. Come ben sottolineato dal *considerando* § 4 del GDPR, laddove si afferma che «[i]l trattamento dei dati personali dovrebbe essere al servizio dell'uomo», vero fruitore ultimo dei benefici tecnologici, anche la scelta di una tecnologia piuttosto che un'altra non è mai neutrale, bensì è sviluppata e adottata, da chi se ne serve, entro la cifra assiologica della dignità della persona[103]. In questa prospettiva, la soluzione va ricercata quindi nella scelta "democratica" della tecnologia più trasparente da utilizzare, in modo da fugare i pericoli della «dittatura dell'algoritmo»[104].

[103] Cfr. R. SENIGAGLIA, *Il dovere di educare i figli nell'era digitale*, in *Persona e mercato*, 3, 2021, p. 525, per il quale «(…) la necessità di definire il rapporto tra l'uomo e la tecnica digitale all'insegna della conformazione di quest'ultima direttamente ad opera di chi la pone: attraverso (i) regole che la rendano compatibile con la dignità dell'uomo, (ii) meccanismi tecnici di controllo (mediante il ricorso agli stessi algoritmi), (iii) mezzi idonei a renderla controllabile e sanzionabile da tutti gli utenti».

[104] S. RODOTÀ, *Il diritto di avere diritti*, cit., p. 402, dove «scompare la persona in sé considerata, trasformata in oggetto di poteri incontrollabili».

Il volume - che fa seguito all'omologo Annuario 2021 - contiene contributi di docenti e ricercatori di varie Università italiane su una pluralità di tematiche che sollecitano la riflessione circa la tenuta delle categorie giuridiche tradizionali a cospetto delle trasformazioni dei modelli di relazione recate dalle tecnologie digitali. Gli scritti sono maturati nel contesto delle attività di ricerca e seminariali promosse dall'Osservatorio Giuridico sulla Innovazione Digitale (OGID), costituito presso il Dipartimento di Diritto ed economia delle attività produttive dell'Università Sapienza di Roma.

I curatori dell'opera, **Salvatore Orlando** e **Giuseppina Capaldo**, sono professori ordinari di diritto privato presso il Dipartimento di Diritto ed economia delle attività produttive di Sapienza Università di Roma.

ISBN 978-88-9377-256-3

www.editricesapienza.it