Università
Ca'Foscari
Venezia

Corso di Dottorato di Ricerca

in Diritto, Mercato e Persona

Ciclo XXXIV

Tesi di Ricerca

La trasparenza algoritmica nel trattamento dei dati personali

Prospettive eurounitarie e statunitensi

SSD: IUS/01

Coordinatore del Dottorato
ch. prof.ssa Claudia Irti

Supervisore
ch. prof.ssa Carmelita Camardi

Dottoranda
Camilla Tabarrini
Matricola 956437

INDICE

INTRODUZIONE

Il presente studio propone una riflessione, sviluppata su tre livelli, del quadro giuridico europeo e statunitense in punto di diritto alla comprensibilità dei processi decisionali automatizzati.

Il primo livello è rappresentato dall'inquadramento della natura giuridica della relazione che si instaura tra titolare del trattamento e soggetto interessato per effetto dell'integrazione di una delle basi giuridiche di cui agli artt. 6 e 9 Reg. (UE) 679/2016 (GDPR). In quest'ottica, il primo capitolo pone le premesse dogmatiche e imposta i termini giuridici delle riflessioni che, al termine del secondo capitolo, porteranno a ragionare sul diritto del soggetto interessato di accedere al proprio profilo. Ripercorrendo i tratti salienti dell'autorevole dibattito sviluppatosi attorno al tema della natura giuridica del dato personale, si sposterà progressivamente l'attenzione sulla posizione giuridica soggettiva che il titolare del trattamento viene a vantare sul dato per effetto del graduale processo di reificazione che lo interessa dalla raccolta, all'aggregazione automatizzata tipica del contesto Big Data, fino alla sua trasformazione in *output* di sistemi di intelligenza artificiale (IA). Tale premessa, infatti, è imprescindibile per impostare correttamente quel bilanciamento tra il diritto ad avere informazioni significative sulla logica seguita dal sistema di IA *ex* art. 22 GDPR e il diritto del titolare del trattamento allo sfruttamento economico dello stesso, sotteso all'intero impianto del Reg. n. 679/2016.

Si procederà quindi per ipotesi, cercando di qualificare giuridicamente quella posizione di vantaggio che il GDPR riconosce in capo al titolare del trattamento attraverso una rilettura delle tradizionali teorizzazioni di stampo realista, industrialista e obbligatorio assumendo, quale angolo prospettico privilegiato, le facoltà riconosciute dal regolamento al titolare. Tali riflessioni, infatti, aiuteranno anche a porre le basi ermeneutiche su cui costruire gli elementi essenziali della relazione negoziale che soggetto interessato e titolare vengono ad intrattenere con riferimento non tanto al singolo dato isolatamente considerato, quanto al metadato inferito in modo automatizzato per effetto di processi di c.d. clusterizzazione e utilizzato (anche) per prendere decisioni nei confronti dei singoli interessati.

Si approda così al cuore dell'analisi, dedicata alla storia, agli elementi costitutivi e al contenuto del diritto alla spiegazione delle decisioni unicamente automatizzate.

Il secondo capitolo, infatti, prende le mosse dai prodromi normativi che hanno preceduto l'attuale formulazione dell'articolo 22 GDPR al fine di meglio chiarirne la portata e, soprattutto, la *ratio* ispiratrice. Per tal via, si proseguirà mettendo meglio a fuoco il contesto (anche tecnologico) nel quale si è venuta affermando l'esigenza di una c.d. vigilanza degli algoritmi, al fine ultimo di porre l'accento su quelle caratteristiche di opacità e complessità con cui si devono inevitabilmente confrontare il legislatore e l'interprete nel decifrare il contenuto e la portata dei doveri/diritti informativi disciplinati dagli artt. 13-15 e 22 GDPR.

Chiarita così l'evoluzione normativa e dottrinale che ha portato la dottrina maggioritaria a riconoscere l'esistenza di un diritto alla spiegazione, si proseguirà offrendo una ricostruzione dettagliata di tutti i suoi elementi costitutivi e, soprattutto, del suo contenuto. È su quest'ultimo, infatti, che si è concentrata l'incertezza interpretativa stante la difficoltà a chiaramente definire i contorni di quella soglia di c.d. significatività fissata dal legislatore eurounitario nel disciplinare le informazioni che il titolare del trattamento è tenuto a rendere all'interessato a fronte dell'assunzione di decisioni unicamente automatizzate nei suoi confronti. Molteplici sono le ricostruzioni dottrinarie prese in considerazione nel compiere il principale sforzo ermeneutico dello studio: tratteggiare in termini operativi i contorni giuridici della spiegazione significativa. Allo scopo, si entrerà nel merito di quel bilanciamento tra posizioni giuridiche contrapposte (soltanto impostato nel primo capitolo) soprattutto con riguardo ai limiti posti dai diritti di proprietà intellettuale che possono di volta in volta venire in rilievo a seconda del contenuto che si attribuisce alla spiegazione.

Conclusa quindi la ricognizione del quadro normativo europeo di riferimento, e avanzate proposte ermeneutiche per la formulazione operativa di spiegazioni significative, la prospettiva dello studio muta nuovamente e si approda così al terzo livello di analisi sulla comprensibilità dei processi decisionali automatizzati: il raffronto comparatistico con l'ordinamento statunitense.

Il terzo capitolo, infatti, mira ad offrire una panoramica del rilevante stato dell'arte legislativo statunitense sia a livello federale che statale. In particolare, compiute le

necessarie premesse storiche e comparatistiche volte a meglio inquadrare il contesto valoriale e normativo in cui si innesta il quadro legislativo e giurisprudenziale di riferimento, l'analisi si sposterà sulle lacune lasciate dal tradizionale standard della *reasonable expectation of privacy* (c.d. *Katz test*) nel contesto digitale e di come sia potenzialmente neutralizzato dall'altrettanto tradizionale principio della *third party doctrine*. Preso atto dell'insoddisfacente contributo del formante giurisprudenziale, ci si sposterà su quello legislativo ricercando spunti di riflessione e possibili linee evolutive nella disciplina dettata dal *Wiretap Act* in punto di analisi automatizzata del contenuto di comunicazioni elettroniche e, in ambito finanziario, dal *Fair Credit Reporting Act* e dall'*Equal Credit Opportunity Act*.

Il carattere settoriale e sostanzialmente lacunoso della disciplina legislativa federale imporrà, tuttavia, una ricognizione delle potenzialità applicative mostrate dalla casistica giurisprudenziale sulla *due process clause* che, seppur mostrando limiti ben maggiori del diritto alla spiegazione disciplinato dal GDPR, offre comunque interessanti spunti di riflessione sullo stretto rapporto che lo standard di significatività viene ad intrattenere con l'effettività del diritto di difesa dei soggetti interessati.

Si concluderà, infine, con cenni sui più recenti approdi legislativi raggiunti dal legislatore californiano nonché sui progetti di iniziative legislative avanzate a livello federale, i quali, analizzati congiuntamente in ragione delle forti affinità mostrate, seppur silenti in punto di diritto alla spiegazione, offrono importanti scorci sulle possibili linee evolutive della disciplina statunitense in materia di data privacy, fondamentali nel contesto della *Data Governance* internazionale specialmente a seguito dell'annullamento del *Privacy Shield*.

L'obiettivo finale dello studio è, infatti, proprio quello di muovere dal contesto normativo (europeo così come statunitense) in punto di processi decisionali automatizzati per tracciarne delle linee ermeneutiche di sviluppo stante il carattere più o meno marcatamente embrionale e lacunoso di entrambe le discipline. In quest'ottica, un importante esempio di standard normativo trasversale e sensibile alle nuove esigenze tecnologiche è senza dubbio rappresentato dalla recente proposta di Regolamento per regole armonizzate sull'Intelligenza Artificiale, al quale verranno dedicate brevi riflessioni conclusive.

CAPITOLO PRIMO

BREVI RIFLESSIONI SULLA NATURA GIURIDICA E L'OGGETTO DEL DIRITTO A TRATTARE I DATI PERSONALI ALTRUI NELLA DISCIPLINA DEL GDPR

SOMMARIO: 1.1. La natura giuridica del dato personale nel quadro della teoria dei beni – 1.2. La funzione sociale del dato personale tra persona e mercato – 1.3. Il "diritto" al trattamento dei dati personali – 1.4. La proprietà dato personale nel quadro del neo-realismo informativo – 1.5. Una prospettiva industrialista: dal diritto morale d'autore alla "quasi proprietà" (intellettuale) sul dato personale – 1.5.1. Cenni di quasi proprietà sui metadati (rinvio) – 1.6. Il trattamento lecito come fonte di obbligazioni "fiduciarie" sui dati personali altrui

1.1. La natura giuridica del dato personale nel quadro della teoria dei beni

L'articolo 810 c.c. definisce "bene" come ogni cosa suscettibile di formare oggetto di diritti[1].

La scelta di aprire la disamina della disciplina sulla comprensibilità dei processi decisionali automatizzati con tale norma si giustifica in ragione dell'adozione di un impianto metodologico che, come osservato da Pugliatti, "partendo dalla impostazione tradizionale, per estendere l'indagine verso la periferia […] presenta il vantaggio della

[1] Sulla teoria generale dei beni giuridici, senza pretesa di esaustività e a titolo meramente esemplificativo, si richiamano S. PUGLIATTI, Cosa (voce), *Enc. dir*., XI, Milano, Giuffré, 1962, 19ss; ID., Beni (voce) (teoria generale), Enc. dir., Vol. V, Milano, Giuffré, 1959, 164ss; O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, Vol. 32, Milano, Giuffrè, 1982; B. BIONDI, *I beni*, in F. VASSALLI (diretto da), *Trattato di diritto civile italiano*, Vol. IV.1, Torino, 1953, 5ss; V. ZENO-ZENCOVICH, Cosa (voce), *D. Disc. Priv*., sez. Civ., IV, 1989, 453 ss; R. FRANCESCHELLI, L'oggetto del rapporto giuridico, *Riv. Trim. dir. proc. civ*., 1957, 1ss; C. MAIORCA, Beni (voce), *Enc. giur. Treccani*, Vol. V, Roma, 1988, 1ss; P. RESCIGNO, *Disciplina dei beni e situazioni della persona*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, V-VI.II, 1976/77, 861ss; C. MAIORCA, Cose (voce), in Enc. giur. Treccani, Vol. XI, Roma, 3ss; A. PINO, Contributo alla teoria giuridica dei beni, *Riv. Trim. dir. proc. civ*., 1948, 825ss.

maggiore sicurezza e concretezza dell'impostazione […]: sì che l'estensione dell'angolo visuale e la generalizzazione dei concetti si può effettuare senza il rischio di apriorismi e di affermazioni non controllate che, riferendosi alle premesse, vizierebbero tutto lo svolgimento della trattazione"[2]. In quest'ottica, la breve ricognizione dell'"impostazione tradizionale" della teoria dei beni è strumentale al preliminare inquadramento dogmatico del dato personale, il quale, come si vedrà meglio a breve, singolarmente considerato nella sua dimensione di mercato, è qui assunto ad "angolo visuale" privilegiato e punto di origine di quel processo di "estensione" ermeneutica (*rectius* specificazione) che approderà, alla fine del prossimo capitolo, alla riflessione sul regime di accesso al *profilo* quale prodotto artificiale della metabolizzazione automatizzata di quel Volume Variegato e Veloce di dati personali noto come *Big Data*[3] e contenuto di quel diritto ad una spiegazione significativa della decisione automatizzata presa nei propri confronti ai sensi dell'articolo 22 del Reg. (UE) 679/2016, norma protagonista dell'analisi successivamente condotta[4].

Seppur il presente studio abbia ad oggetto la relazione giuridica tra il titolare e l'interessato nelle circostanze or ora indicate, siffatta premessa metodologica rende obbligata una preliminare riflessione sulla natura giuridica del dato personale alla luce del risalente e autorevole dibattito dottrinale originato dall'ambiguo utilizzo legislativo del termine "cosa" e dalla sua relazione, più o meno biunivoca, con l'affine concetto di "bene" in senso giuridico[5]. Come noto, infatti, la dottrina prevalente distingue tra una

[2] S. PUGLIATTI, Cosa (voce), cit., §6.

[3] Cfr. M. N. HELVESTON, Consumer Protection in the Age of Big Data, 93, *Wash. U. L. Rev*., 2016, 859, 867; G. D'ACQUISTO e M. NALDI, *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli Editore, Torino, 2017, 12ss; T. CALDERS e B. CUSTERS, What is Data Mining and How Does it Work? in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society*. *Data Mining and Profiling in Large Databases*, Springer, New York, 2013, 28; ZENO-ZENCOVICH, Ten Legal Perspectives on the "Big Data Revolution", 1, *Concorrenza e mercato*, 29, 2016, 29; E. PELLECCHIA, Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR, *NLCC*, 2, 2020.

[4] Il collegamento tra la disciplina del dato, seppure non personale e genericamente riguardato come peculiare declinazione del concetto di informazione, e la disciplina dei processi decisionali è stato già da tempo autorevolmente messo in luce, osservando come "[u]n ultimo aspetto, in parte connesso con quelli trattati nei paragrafi precedenti, riguarda la possibilità di accedere a talune informazioni che non riguardano sé medesimi e sono detenute da terzi. Quali? Nelle democrazie occidentali ha assunto negli ultimi decenni un crescente valore il principio della trasparenza dei processi decisionali, in primo luogo di quelli pubblici o di rilevanza pubblica. Si tratta di un valore che ha trovato fertile terreno nei paesi anglosassoni, per un verso più inclini a favorire la partecipazione dei cittadini alle decisioni pubbliche, per altro verso non impacciati dalla secolare tradizione continentale dell'intangibilità e segretezza della sfera amministrativa." V. ZENO-ZENCOVICH, Informazione (profili civilistici) (voce), *Digesto Disc. Priv.*, Sez. civ., Vol. IX, Torino, 1993, 421ss.

[5] La disomogeneità che trapela da una lettura sistematica degli utilizzi dei termini "bene" e "cosa" nei vari libri del Codice civile lascia intravedere la mancanza di una chiara e coerente *intentio legis* dalla

nozione di "bene" che, in quanto "eminentemente giuridica" e formale, prescinderebbe dalla dimensione fisica del suo oggetto arrivando a ricomprendere qualsiasi "entità [materiale o immateriale] oggetto di un interesse giuridicamente tutelato" [6], e una nozione pre o extra giuridica di "cosa" intesa come "entità obiettiva"[7] che, in virtù di retaggi romanistici[8], si contraddistinguerebbe per il carattere della corporalità[9]. Ne consegue che,

quale, tuttavia, emerge una tendenziale (seppure non univoca) distinzione tra la nozione di "cosa" e quella più ampia di "beni", spesso ricomprendenti entità quali crediti, debiti e avviamento. In tal senso, l'analitica ricognizione autorevolmente condotta da Zeno-Zencovich mette in luce come, ad esempio, alla tendenziale equiparazione tra bene e cosa del libro sesto del codice civile, si contrapponga la ricorrente distinzione che il libro quarto opera, spesso implicitamente, tra la corporalità associata alle "cose" e la potenziale immaterialità dei "beni", ben esemplificata dal richiamo ad attività e crediti operato dalla disciplina della cessione dei beni ai creditori. Assimilazione, quest'ultima, a sua volta contraddetta dalla distinzione che invece altre norme operano tra beni e crediti (e.g. artt. 2343, 2476, 2518, etc.). V. ZENO-ZENCOVICH, Cosa (voce), *cit*., §2.

[6] V. ZENO-ZENCOVICH, Cosa (voce), *cit*., §4. *Contra* B. BIONDI, I beni, *cit*., 13-16 che assimila il bene all'interesse oggetto del diritto soggettivo. Cfr. G. PUGLIESE, Diritti reali (voce), *Enc. dir*., XII, Milano, Giuffré, 1964, 755ss; ID., Dalle «res ìncorporales» del diritto romano ai beni immateriali di alcuni sistemi giuridici odierni, *Rivista Trimestrale di Diritto e Procedura Civile*, 4, 1982, 1137ss,; M. COMPORTI, *Diritti reali in generale*, in A. CICU, F. MESSINEO, L. MENGONI, (già diretto da) e P. SCHLESINGER (continuato da), *Trattato di diritto civile e commerciale*, II ed., Milano, Giuffré, 2011, 49 ss; C. MAIORCA, *La cosa in senso giuridico. Contributo alla critica di un dogma*, Napoli, Edizioni Scientifiche Italiane, 1978 (ristampa), 14ss; S. PUGLIATTI, Beni (voce) (teoria generale), *cit*., §8; A. LEVI, *Teoria generale del diritto*, Padova, Cedam, 1967, *passim*; D. MESSINETTI, *Oggettività giuridica delle cose incorporali*, Milano, Giuffré, 1970, *passim*.; O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, *cit*., 39ss.

[7] Più precisamente, la cosa in senso pregiuridico è stata definita come "porzione della realtà, in quanto contrapposta ai soggetti che in essa operano o che la conoscono e identificata nel rispetto alla circostante realtà obiettiva". Così M. ARE, Beni immateriali (voce), *Enc. dir*., V, Milano, Giuffré, 1959, 244ss.

[8] Il riferimento è alla canonica distinzione tra *res corporales* e *res incorporales* tratteggiata da Gaio nelle sue Istituzioni e che, nella sua interpretazione letterale, contrapponeva le "cose che si possono toccare" ai diritti (*rectius* le cose che "*in iure consistunt*"). L'aporia prodotta da tale apparente sovrapposizione tra il piano del diritto e quello del suo oggetto stimolò un chiarimento ermeneutico volto a precisare come, in realtà, identificando il diritto con la cosa che ne forma l'oggetto, Gaio avesse voluto distinguere tra cose (corporali) su cui si esercita il diritto di proprietà e altre cose su cui si esercitano diritti diversi. Di qui l'affine tradizione civilistica di assimilazione della posizione dominicale all'esercizio di una signoria su beni materiali. Cfr. S. PUGLIATTI, Cosa (voce), cit., § 10; V. ZENO-ZENCOVICH, Cosa (voce), *cit*., §11.

[9] Per una nozione di cosa come qualsiasi oggetto corporale o altra entità naturale suscettibile di appropriazione o utilizzazione si veda F. MAROI, Cosa (voce), *Nuovo dig. it.*, IV, Torino, Utet, 1938, 356ss. In senso analogo A. BUTERA, *Il Codice civile italiano*. *Libro della proprietà*., pt. I, Torino, 1941, 19ss. Degrada, invece, a distinzione meramente linguistica quella tra beni e cose, concependo i termini come sinonimi, B. BIONDI, I beni, *cit*., 9 e 15.Per un rapporto tra cosa e bene in termini di genere a specie si veda G. DE SEMO, *Istituzioni di diritto privato*, V ed., Firenze, G. Barbèra, 1948, 167ss.

a differenza di quanto avviene in altri ordinamenti[10], le "cose in senso giuridico"[11], intese come "porzione della realtà obiettiva in cui si esplica quel comportamento dei soggetti cui la norma riferisce le sue valutazioni"[12], costituiscono soltanto una parte dei beni in senso giuridico: la porzione di beni materiali oggetto del diritto di proprietà (o di altri diritti reali) nella sua prevalente declinazione di matrice romanistica[13]. Accanto a questi, quindi, vengono a configurarsi "altre entità suscettibili di essere qualificate come beni" in quanto "punto di riferimento di precisi interessi giuridici cui è offerta una primaria ed articolata protezione da parte dell'ordinamento" e tradizionalmente riconducibili alla categoria del c.d. pensiero estrinsecato confluita poi nella più ampia nozione di beni immateriali[14].

La variegata pletora di beni nel tempo progressivamente ascritta a tale ultima categoria ha reso però l'attività dottrinale di definizione del concetto di bene immateriale particolarmente complessa[15]. Ciononostante, l'insufficienza dogmatica di una prospettiva definitoria meramente negativa, tesa a individuare l'unico tratto caratterizzante della fattispecie nell'assenza di fisicità, ne ha stimolato una più puntuale perimetrazione ermeneutica volta a ricomprendere nella nozione di beni immateriali (in senso giuridico)

[10] Nell'ordinamento tedesco la qualificazione giuridica di bene è normativamente legata al carattere della materialità dell'oggetto. Al contrario, i legislatori di Austria e Scozia sono tra i più "liberali" a livello europeo, avendo adottato una nozione residuale di "cosa" tale per cui vi rientra tutto ciò che non è giuridicamente qualificabile con "persona". Non in tutti gli ordinamenti, quindi, il carattere della materialità è indispensabile per poter qualificare un bene come "cosa" in senso giuridico. Cfr. A. BOERDING, N. CULIK, C. DOEPKE, T. HOEREN, T. JUELICHER, C. ROETTGEN, M.V. SCHOENFELD, Data Ownership. A Property Rights Approach from a European Perspective, 11, *Journal of Civil Law Studies*, 2, 2018, 323, 338. Interessante, a tal riguardo, la nozione di merce fatta propria dalla Corte di giustizia dell'Unione europea in termini di prodotto suscettibile di valutazione monetaria e potenziale oggetto di scambi commerciali. Sentenza della Corte del 10 dicembre 1968, Commissione delle Comunità europee contro Repubblica italiana, Causa 7-68 (ECLI:EU:C:1968:51).

[11] Sulla necessità di un'interposizione legislativa a segnare il passaggio tra la cosa in senso pre-giuridico e cosa in senso giuridico (*rectius* a cui l'ordinamento ha attribuito rilevanza giuridica) v. R. NICOLÒ, *L'adempimento dell'obbligo altrui*, Vol. X, Napoli, Edizioni Scientifiche Italiane, 1978 (ristampa), 78; A. PINO, Contributo alla teoria giuridica dei beni, *cit.*, 833.

[12] M. ARE, voce Beni immateriali, *cit.*, § 2.b.

[13] Cfr. V. SCIALOJA, *Teoria della proprietà nel diritto romano*, Vol. I, Roma, Attilo Sampaolesi, 1928, 29ss. Per riflessioni critiche sull'adattabilità dello schema dei diritti reali a rapporti con beni immateriali v. M. COMPORTI, *Diritti reali in generale*, *cit.*, 130ss. Sottolinea, invece, lo stretto rapporto tra la materialità della cosa che ne forma oggetto e il carattere assoluto, immediato ed esclusivo del diritto di proprietà sullo stesso S. PUGLIATTI, *La proprietà nel nuovo diritto*, II ed., Milano, Giuffré, 1964, 250 ss. In senso analogo O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, *cit.*, 190ss. *Contra* S. SATTA, Cose e beni nell'esecuzione forzata, 9-10, *Rivista del diritto commerciale*, 1964, 350, 354.

[14] Cfr. V. V. ZENO-ZENCOVICH, Cosa (voce), *cit.*, § 8; M. BARCELLONA, Attribuzione normativa e mercato sulla teoria dei beni giuridici, *Quadrimestre*, 1987, 607, 610ss; D. MESSINETTI, Beni immateriali (voce), *Enc. giur. Treccani*, V, Roma, 1988, 1ss.

[15] Sul carattere "disorganico e contraddittorio" della categoria dei beni immateriali R. FRANCESCHELLI, *Beni immateriali*, Torino, Utet, 1960, 394ss.

soltanto quelle cristallizzazioni obiettivate e circolabili del pensiero soggettivo individuale, fissato in un dato momento del suo divenire e perciò distinto dal suo autore (c.d. entità -pregiuridiche- di pensiero o intellettuali), prese in considerazione dal diritto "ai fini della concessione di una tutela esclusiva, facendone oggetto conseguentemente di rapporti o di situazioni giuridiche[16]."

Assumendo le classificazioni sin qui brevemente rievocate a quadro dogmatico di riferimento, è quindi possibile giungere alla preliminare conclusione per cui il dato personale, in quanto entità intellettuale dotata dei caratteri della "astrattezza, circolabilità, riproducibilità", nonché del "carattere di plurimo e contemporaneo integrale godimento"[17], ed in quanto oggetto delle situazioni giuridiche soggettive orbitanti attorno alla fattispecie legislativamente disciplinata del trattamento dei dati personali, non potrebbe che configurarsi come bene immateriale e, quindi, in quanto tale, suscettibile di utilizzazione ma non di appropriazione[18].

Senonché tale conclusione non può che infrangersi contro il carattere tipico e tassativo di tale categoria. I beni immateriali assurgono quindi a mero parametro dogmaticamente descrittivo di entità giuridiche che sono state perciò autorevolmente ricondotte alla macrocategoria dei cc.dd. beni intangibili[19]. In tale più ampia nozione, infatti, oltre ai beni immateriali, sono state autevorevolmente annoverate anche quelle entità di origine amministrativa "inimmaginabili al di fuori della regolazione delle Autorità"[20] in quanto prodotto di un processo regolatorio che contestualmente crea un

[16] Più precisamente, e analogamente a quanto già visto con riferimento alla nozione di cosa (materiale) in senso giuridico, la "categoria giuridica dei beni intellettuali o immateriali, non [è] composta da tutte le entità intellettuali ma da quelle sole che il diritto prende in considerazione ai fini della concessione di una tutela esclusiva, facendone oggetto conseguentemente di rapporti o di situazioni giuridiche. Per modo che è esatto, giuridicamente e logicamente, attribuire alle entità intellettuali prese in considerazione dal diritto, la qualifica di beni intellettuali, o, volendo seguire la terminologia tradizionale, immateriali." (corsivo omesso) M. ARE, Beni immateriali (voce), *cit*., § 3. Definisce, invece, i beni immateriali come "creazioni intellettuali che siano oggetto di un diritto assoluto" R. FRANCESCHELLI, *Beni immateriali*, *cit*., 421. Cfr. C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Giappichelli Editore, Torino, 2020, *passim*; C. CAMARDI, Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali, 3, *Giustizia Civile*, 2019, pp. 499ss

[17] M. ARE, Beni immateriali (voce), § 5.

[18] Sul carattere immateriale, non rivale e, quindi, non esclusivo del dato personale cfr. M. OREFICE, I *Big Data*. Regole e concorrenza, 4, *Politica del diritto*, 2016, 697 ss; V. ZENO-ZENCOVICH, Ten Legal Perspectives on the '*Big Data* Revolution', 1, *Concorrenza e Mercato*, 2016, 29ss; S. SCHAFF, La nozione di informazione e la sua rilevanza giuridica, 2, *Diritto dell'informazione e dell'informatica*, 1987, 445, 450ss.

[19] C. CAMARDI, Cose, beni e nuovi beni, tra diritto europeo e diritto interno, 3, *Europa e diritto privato*, 2018, 955 ss, *passim*.

[20] *Ivi*, 1016.

bene[21] e la relativa situazione soggettiva di appartenenza, sulla quale si incardina poi il mercato secondario di circolazione del bene intangibile di riferimento[22]. Sebbene i dati personali non siano pienamente assimilabili neppure a tale nozione di cc.dd. beni di creazione amministrativa, si ritiene che cionondimento siano parimenti riconducibili alla medesima macrocategoria dogmatica dei beni intagibili. Il GDPR, infatti, nel disciplinare le condizioni (*rectius* basi giuridiche) per il trattamento legittimo dei dati personali e nel definire i diritti e doveri che per l'effetto scaturiscono in capo al titolare del trattamento e ai soggetti interessati, crea un sistema di circolazione del dato-bene intangibile caratterizzato da un proprio regime giuridico e da peculiari posizioni giuridiche soggettive.

È proprio sulla qualificazione della natura e del contenuto della situazione giuridica soggettiva di appartenenza del bene intangibile-dato personale che si concentrerà quindi il proseguo del capitolo. Ciò in quanto, se è vero che il dato personale è una *species* di quel *genus* informazione tradizionalmente riguardata come "qualsiasi dato rappresentativo della realtà che viene conservato da un soggetto oppure comunicato da un soggetto ad un altro"[23], è altrettanto vero che il frammento di realtà rappresentato

[21] Nella sua accezione di oggetto di tutela in senso obiettivo, v. S. PUGLIATTI, *Beni e cose in senso giuridico*, Milano, Giuffré, 1962, 24ss.

[22] *Ivi*, 1018. Cfr. G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, Torino, Utet, 2010; A. ZOPPINI, Le «nuove proprietà» nella trasmissione ereditaria della ricchezza (note a margine dellateoria dei beni), 2, *Riv. Dir. Civ*., 2000, 185ss.

[23] V. ZENO-ZENCOVICH, Informazione (profili civilistici) (voce), *cit.*, §1. Per una distinzione tra singoli dati intesi come "*patterns with no meaning*" e informazioni riguardate come "*interpreted data that has meaning*" v. L. DETERMANN, No One Owns Data, 70, *Hastings L.J.*, 1, 2018, 3, 6-7 ove richiama le analoghe riflessioni compiute da S. BAŠKARADA, A. KORONIOS, Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and Its Quality Dimension, 18, *Australasian J. Info. Sys*., 1, 5, 7. A tal riguardo, interessanti anche le riflessioni di BRAVO, secondo il quale "un solo dato non costituisce un'informazione, la quale può aversi dalla correlazione di almeno due di essi. In tal senso, quando si parla di "dato personale" non si fa riferimento al dato in sé, ma sempre ad una informazione, in quanto l'espressione suddetta ("dato personale") presuppone la riferibilità del dato ad una persona e, dunque, la correlazione di almeno due dati, che consente di ricavare elementi informativi riferibili ad un soggetto determinato o determinabile". ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018, 43, spec. nt. 2. In senso analogo si esprime C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 60 secondo cui "si può affermare che il dato è la fonte dell'informazione, nel quale questa è contenuta e dal singolo dato o dall'insieme di dati l'informazione può essere estratta o inferita. Ma l'informazione, a rigore, non coincide con il dato stesso. L'informazione è elaborazione del dato." Cfr. M. HILDEBRANDT, Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics, 68, *U. Toronto L.J.*, 1, 2018, 3 ss e ID., Law as Information in the Era of Data-Driven Agency, 79, *Mod. L. Rev*., 2016, 1ss; P. PERLINGERI, *L'informazione come bene giuridico*, in ID. (a cura di), *Il diritto dei contratti fra persona e mercato*, Napoli, Edizioni Scientifiche Italiane, 2003, 333ss; ID., L'informazione come bene giuridico, 2, *Rassegna di diritto civile*, 1990, 326ss; V. ZENO ZENCOVICH, Sull'informazione come "bene" (e sul metodo del dibattito giuridico), 17, *Riv. crit. dir. priv*., 3, 1999, 485ss; D. MESSINETTI, Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali, 16, *Riv. crit. dir. priv*., 3, 1998, 339ss;

dal dato personale si contraddistingue per l'essere riferibile ad "una persona fisica identificata o identificabile"[24].

Ciononostante, ammettere che il dato personale, in quanto informazione rappresentativa di un frammento dell'identità del soggetto interessato, sia oggetto di un diritto della personalità, non significa negarne la natura di bene in senso giuridico poiché, come autorevolmente osservato, anche i diritti personali "garantendo al soggetto titolare la tutela specifica di determinati interessi, danno luogo alla nascita di beni in senso giuridico"[25], da intendersi, ai fini delle riflessioni in esame, non come cose, né risorse immateriali (nel senso in cui il legislatore le intende e disciplina) e neppure come invenzioni suscettibili di utilizzo industriale (sul punto peraltro si dirà meglio in seguito) ma, appunto, come beni intangibili nel senso appena descritto.

In secondo luogo, la presa d'atto della natura di bene in senso giuridico del dato personale (*rectius* bene intangibile) in quanto oggetto di un diritto della personalità, non esclude che il dato stesso, pur se unitario nella sua dimensione pregiuridica di entità immateriale, possa formare contestualmente oggetto di altri e diversi diritti soggettivi, in presenza di determinate circostanze, dando vita ad altrettanti autonomi beni in senso giuridico[26].

A. NERVI, La nozione giuridica di informazione e la disciplina di mercato. Argomenti di discussione, *Riv. dir. comm*., 1998, 843ss.

[24] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE G.U. L119/1 [d'ora in avanti GDPR], Articolo 4.

[25] S. PUGLIATTI, Beni (voce) (teoria generale), *cit*., § 11.

[26] In particolare, nelle parole dell'Autore: "[l]a cosa, nella sua individualità obbiettiva, è una e identica; ma, in quanto oggetto giuridico, assume vari aspetti: altro è come oggetto della proprietà, altro come oggetto dell'usufrutto; e ancora: altro come oggetto dell'ipoteca sulla nuda proprietà, altro come oggetto dell'ipoteca sull'usufrutto. Diversi sono, Infatti i diritti che vengono a costituirsi con riferimento all'unica cosa; diversi gli interessi o le utilità che l'ordinamento giuridico tutela, e le facoltà di utilizzazione e di sfruttamento della cosa che la legge prende in considerazione nel foggiare i singoli diritti quali strumenti di tutela per i soggetti che ne sono i destinatari. […] *Ciò appare evidente in ordine ai diritti reali, ma non è dubbio che analoghe considerazioni debbano valere per i diritti personali. Anche questi, infatti, garantendo al soggetto titolare la tutela specifica di determinati interessi, danno luogo alla nascita di beni in senso giuridico*." (corsivo aggiunto) IBID. Dal canto suo, ARE identifica il termine bene con la cosa in senso giuridico, e lo definisce come "il fine pratico costituente l'oggetto della tutela giuridica, concessa mediante l'attribuzione di un diritto al soggetto." Viene così a configurarsi la possibilità di concepire "una pluralità di beni formali, in relazione alla medesima *res* sostanziale, in corrispondenza ad una eventuale molteplicità di diritti in ordine alla *res* stessa ed alla conseguente pluralità di fini determinati, per tal modo riceventi specifica ed autonoma tutela." In quest'ottica, quindi, il bene diventa espressione di uno dei potenzialmente molteplici diritti sulla cosa specificatamente e autonomamente tutelati dall'ordinamento. M. ARE, Beni immateriali (voce), *cit*., § 2. Per un ammonimento sul rischio ermeneutico di confusione tra interesse e bene v. F. CARNELUTTI, *Usucapione della proprietà industriale*, Milano, Giuffré, 1938, 53ss.

Siffatta conclusione, peraltro, si rende tanto più necessaria rispetto allo specifico bene giuridico del dato personale nella misura in cui, ove esclusivamente riguardato come "proiezione esterna della personalità" del soggetto interessato a cui si riferisce e non come un "*quid* oggettivato" e distinto dallo stesso, renderebbe sì l'informazione in esso contenuta oggetto di tutela, ma soltanto in via mediata e strumentale alla salvaguardia del diritto soggettivo assoluto alla protezione dei dati personali dei soggetti interessati nella sua esclusiva dimensione di diritto della personalità assurgendo, quindi, a mero strumento alternativo di tutela della persona[27].

Tale impostazione, tuttavia, per quanto dogmaticamente impeccabile, risulta anche inevitabilmente parziale poiché, relegando in una dimensione meramente accidentale e accessoria il valore di scambio (se non propriamente patrimoniale) assunto dal dato personale, trascura la conformazione di mercato oggi assunta dal fenomeno giuridico della circolazione del dato personale[28] e, di conseguenza, condanna l'interprete che cerca di regolarlo a cadere in una ineludibile contraddizione in termini.

Ai fini dell'analisi che segue è quindi imprescindibile focalizzare temporaneamente l'attenzione sul dato personale nella sua declinazione di bene giuridico

[27] In altri termini, "l'informazione non è, in genere, tutelata in quanto tale bensì in via mediata, quando assume rilievo per la personalità del soggetto oppure assurge al rango di un bene, diverso, già tutelato dall'ordinamento." Così V. ZENO-ZENCOVICH, Cosa (voce), *cit*., § 13. E, ancora, "convincente — e generalmente già recepita — è la qualificazione del diritto di esclusiva sui propri dati personali come diritto della personalità e più precisamente come espressione della riservatezza. Il soggetto è tutelato da intrusioni fisiche o tecnologiche nel suo domicilio, dalla riproduzione non autorizzata delle proprie sembianze fisiche nonché dall'appropriazione di alcune categorie di dati ritenuti «sensibili». Ciò significa — per tornare al discorso di partenza — che non è l'informazione in sé ad essere oggetto di disciplina, quanto la circostanza che essa è rivelatrice di aspetti già protetti". ID., Informazione (profili civilistici) (voce), *cit*., § 5. Cfr. G. ALPA, *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessione sul GDPR*, Padova, Cedam, 2019, 9 ss; G. GIAMPICCOLO, La tutela giuridica della persona umana e il c.d. diritto alla riservatezza, *Riv. trim. dir. e proc. civ*, 2, 1958, 458ss; G.B. FERRI, *Persona e formalismo giuridico*, Rimini, Maggioli Editore, 1987, 337ss; V. ZENO ZENCOVICH, Personalità (diritti della) (voce), *Dig. disc. priv*., Sez. civ., I, XIII, Torino, 1995, 453ss. Contra, per riflessioni a supporto di una concezione monistica, v. A. DE CUPIS, *I diritti della personalità*, in A. CICU, F. MESSINEO, L. MENGONI, (già diretto da) e P. SCHLESINGER (continuato da), *Trattato di diritto civile e commerciale*, II ed., Milano, Giuffré, 1982, 44ss; D. MESSINETTI, Personalità (diritti della) (voce), *Enc. dir*., XXXIII, Milano, Giuffré, 1983, 37ss. Cfr. R. ORESTANO, *Azione, diritti soggettivi, persone giuridiche. Scienza del diritto e storia*, Bologna, Il Mulino, 1978, 113ss.

[28] Da ultimo ribadita con la COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia europea per i dati* (Bruxelles, 19 febbraio 2020) (COM(2020) 66 final). Cfr. R. SENIGAGLIA, La dimensione patrimoniale del diritto alla protezione dei dati personali, in *Contratto e Impresa*, 2020, 760 ss; G. D'IPPOLITO, Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale, in *Diritto dell'Informazione e dell'Informatica*, 3, 2020, 634 ss; V. RICCIUTO, La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, in *Diritto dell'Informazione e dell'Informatica*, 4, 2018, 709ss; S. THOBANI, Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente, in *MediaLaws - Rivista di diritto dei media*, 3, 2019, 131-147.

oggetto della diversa situazione giuridica soggettiva, stavolta di matrice squisitamente patrimoniale, facente capo al titolare del trattamento. È soltanto assumendo una prospettiva economica e guardando al dato personale principalmente (seppure non esclusivamente) come bene suscettibile di soddisfare bisogni umani e produrre utilità (*rectius* ricchezza) [29], infatti, che si potrà riflettere, senza pregiudizi dogmatici, sulla natura giuridica della relazione che si instaura tra titolare del trattamento e soggetto interessato per effetto del verificarsi di una delle basi giuridiche di cui agli articoli 6 e 9 Regolamento Generale sulla Protezione dei Dati Personali (d'ora in avanti GDPR)[30].

In altre parole, tra la natura "personale" del dato/informazione (tutelabile come aspetto della protezione della persona) e la sua natura "patrimoniale", che lo rende suscettibile di essere oggetto di diritti di altri, si interpongono la tecnologia e i processi tecnico-giuridici che rendono possibile l'elaborazione dei dati personali in forma professionale, e prima ancora la stessa "nascita" del dato come frammento potenzialmente separabile dalla persona cui afferisce (ciò che in sostanza è reso possibile dalla digitalizzazione). Tutto questo genera quell'insieme di relazioni economiche che sono

[29] Ai tratti dell'utilità e dell'attitudine a soddisfare bisogni umani che autorevole dottrina associa alla nozione di bene, parte della scienza economica aggiunge anche il necessario carattere della limitatezza, nella misura in cui, come già osservato, "se il bene può ottenersi in misura esuberante riguardo ai bisogni e senza sforzo alcuno, non può verificarsi in rapporto ad esso alcun calcolo economico; il consumo di qualsiasi frazione del bene medesimo non può chiamarsi imprevidente, poiché altre frazioni saranno immediatamente disponibili per l'appagamento di qualsiasi desiderio." In quest'ottica, se al carattere della non rivalità del dato, si affianca quello della sua illimitata e agevole riproducibilità, potrebbe dubitarsi della sua natura bene, quantomeno in prospettiva economica. Così A. GRAZIANI, *Istituzioni di economia politica*, IV ed., 1936, 49 citato da S. PUGLIATTI, Beni (voce) (teoria generale), *cit*., § 6.

[30] Senza pretesa di esaustività, si richiamano le recenti riflessioni circa i profili di novità introdotti dal Regolamento offerte da F. DI RESTA, *La nuova 'Privacy europea': i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore, Torino, 2018, 31 ss; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario. Regolamento (UE) 2016/679 del 27 aprile 2016 - Decreto di adeguamento D.Lgs. n. 101/2018 - Codice privacy D.Lgs. n. 196/2003*, Ipsoa, Milano, 2018; F. DE STEFANI, *Le regole della privacy. Guida pratica al nuovo GDPR*, Ulrico Hoepli Editore, Milano, 2018; A. NERVI, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 161 ss; A. SPANGARO, *L'ambito di riferimento materiale del nuovo regolamento*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 23 ss; 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*, Cedam, 2019, 35ss; C. COLAPIETRO e A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO e C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017, 85ss; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679*, Giappichelli Editore, Torino, 2016, 7ss; E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy* , in ID. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 23 ss.

oggetto di regolamentazione da parte della disciplina della privacy e poi del GDPR, e nel contesto delle quali vengono definiti diritti e obblighi delle parti.

Ed è proprio il chiaro inquadramento di tali relazioni interprivate a fornire un'insostituibile chiave di lettura del bilanciamento tra quei contrapposti interessi che, come si vedrà meglio nel prossimo capitolo, vengono a collidere in quella specifica e nuova fattispecie di elaborazione professionale dei dati che sfocia nella spiegazione significativa dei processi decisionali automatizzati di cui all'articolo 22 GDPR.

In altri termini, la razionalizzazione ermeneutica della natura giuridica del dato e, conseguentemente, delle posizioni giuridiche soggettive ad esso riconducibili, è una premessa teorica indispensabile all'analisi del diritto ad una spiegazione dei processi decisionali automatizzati in quanto, plasmando il regime di circolazione della singola informazione, informa anche il regime di accesso alla logica seguita dalla macchina nell'addivenire alla decisione, sia ove intesa come il complesso dei dati che l'hanno "allenata" e "alimentata", sia ove assimilata al profilo assunto a base artificialmente inferita della decisione automatizza.

Allo scopo il capitolo proseguirà, dapprima, mettendo meglio a fuoco le dinamiche di mercato proprie dell'economia dei dati, così da meglio identificare le professionalità e gli interessi in essa coinvolti a seguito dell'affermazione di quei processi tecnico/imprenditoriali prima indicati. Successivamente, inquadrato il bene giuridico (intangibile) "dato personale" alla luce della sua c.d. funzione sociale[31], si procederà con una rapida ricognizione delle principali tesi avanzate rispetto al regime giuridico da applicare alla sua circolazione, strumentale alla formulazione della proposta conclusiva di definizione della situazione giuridica soggettiva in capo al titolare del trattamento ed avente ad oggetto il dato in quanto cristallizzazione estrinsecata di un aspetto della personalità dell'interessato in un dato momento del suo divenire e, perciò, espressivo di una stima approssimativa e temporalmente confinata, della sua personalità.

[31] Così Considerando 4 GDPR.

1.2. La funzione sociale del dato personale tra persona e mercato

Muovendo dalla presa d'atto della natura pregiuridica di entità immateriale del dato personale, e spostando l'attenzione sull'esigenza di meglio definire i contorni di quelle situazioni giuridiche soggettive che, avendolo come oggetto, gli conferiscono rilevanza in senso giuridico, il paragrafo proseguirà mettendo in luce gli aspetti del dato che, in prospettiva sia empirica che giuridica, influiscono sulla configurabilità e configurazione delle prime[32].

Come accennato, la prima caratteristica del dato personale, sul quale si è tradizionalmente concentrata l'attenzione della dottrina, è l'intima relazione che lo stesso, in quanto "proiezione della persona", intrattiene con la dimensione della sua identità, specialmente ove riguardata nella sua declinazione digitale[33].

Sebbene tale connotazione personalistica dell'informazione di cui il dato si fa portatore sia stata per lungo tempo riguardata come l'esclusiva dimensione meritevole di tutela (di qui il differente e nettamente più liberale regime di circolazione riservato al dato anonimizzato[34]), diversa e più recente dottrina, adottando una prospettiva definita "giusrealista"[35], ha prediletto un approccio dogmatico alla ricostruzione della nozione di

[32] Sulla necessità di distinguere, seppure con riferimento al diritto d'autore, il bene immateriale dai diritti che su di esso insistono si veda, fra gli altri, V. DE SANCTIS, Considerazioni giuridiche sulla riforma della legislazione sul diritto d'autore, *Il diritto di autore*, 1940, 239, 242 ss. Cfr. M. BERTANI, *Proprietà intellettuale, antitrust e rifiuto di licenze*, Quaderni di Aida, X, Milano, Giuffré, 2004, 49ss; G. CAVANI, *Oggetto della tutela*, in L.C. UBERTAZZI (a cura di), *Legge sul software. Commentario sistematico*, Quaderni di Aida, I, Milano, Giuffré, 1994, 14ss.

[33] Nelle parole di Alpa: "l'informazione è sì considerata un bene -in questo caso inerente la persona- perché ha ad oggetto un aspetto della persona idoneo ad identificarla; ma non è dunque tutelata in sé e per sé, ma soltanto in ordine al suo contenuto. […] [I]l dato personale, proprio perché legato alla persona, ne compone l'identità digitale, quasi fosse una proiezione della persona stessa, "una sua parte"." G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, 17.

[34] Tale regime è attualmente disciplinato dal 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, GUUE L 303/59. Sulla dinamicità della nozione di dato riferibile ad una persona fisica "identificabile" si vedano le riflessioni condotte da C. IRTI, Dato personale, dato anonimo e crisi del modello normativo dell'identità, 2, *Jus Civile*, 2020, 379, 387, la quale sottolinea come la nozione di anonimità del dato personale fatta propria dal legislatore eurounitario, essendo legata al contesto tecnologico di riferimento, mantiene un certo grado di flessibilità operativa nella misura in cui qualifica come anonimo il dato non soltanto quando sia tecnologicamente impossibile riferirlo ad una persona fisica, ma anche quando tale operazione risulti "ragionevolmente improbabile" perché diseconomica alla luce delle "tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici". Così anche GDPR, Considerando 26.

[35] Cfr. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, *cit.*, 39.

"bene" che, mirando a sanare "lo scollamento del sistema giuridico con la realtà"[36], dia rilevanza giuridica al dato anche in quanto bene suscettibile di utilizzazione [37].

Tale prospettiva si rende ancor più necessaria nel contesto Big Data, dove quel carattere "a due facce" del dato (già messo in luce con riferimento alla disciplina delle banche dati[38]) si è senz'altro esacerbato. L'economia dei dati, infatti, ha reso evidente come, pur mantenendo la natura di diritto fondamentale, il diritto alla protezione dei dati si mostri condizionato, ovvero non assoluto e non necessariamente indisponibile[39]. Di qui l'emersione di quella c.d. funzione sociale che il Considerando 4 del Reg. (UE) 679/2016 riconosce a tale posizione giuridica al fine di ribadire la necessità di un suo proporzionale contemperamento con altri diritti fondamentali[40].

È proprio nella funzione sociale acquisita dal dato nel contesto del mercato digitale, peraltro, che si inquadra più chiaramente quella dinamicità della tutela che Rodotà poneva a *discrimen* tra la disciplina degli articoli 7 e 8 della Carta di Nizza[41] . In quest'ottica, quindi, il diritto alla protezione dei dati personali si è venuto a declinare in una serie di tutele attive volte a consentire all'interessato di seguire il dato nella sua circolazione e che, complessivamente, lo collocano *ab origine* in una prospettiva

[36] G. RESTA, V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, *Riv. Trim. Dir. Proc. Civ.*, 2, 2018, 411ss.

[37] Con riguardo, invece, ad atteggiamenti interpretativi cc.dd. sociologici i.e. "volt[i] a determinare le nozioni di "beni" e di "cosa" sulla base di una tipizzazione dei comportamenti sociali giuridicamente rilevanti" V. ZENO-ZENCOVICH, Cosa (voce), *cit*., § 3.

[38] G. ALPA, *Prefazione*, in A. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Vol. I, Milano, Giuffré, 2003, *passim* richiamato da L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 60.

[39] G. ALPA, *La "proprietà" dei dati personali*, cit., 13-14. In senso analogo, nota come "È […] in relazione agli interessi della riservatezza, dell'identità personale, del controllo sulla circolazione dell'immagine e degli altri segni distintivi della personalità, che si è infranto il mito della dicotomia tra persona e contratto e sono stati recuperati all'autonomia privata molti degli spazi prima negati dalle impostazioni rigidamente pubblicistiche" G. RESTA, La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della carta dei diritti), *Rivista di diritto civile*, 2002, 801, 817.

[40] Nonostante la varietà delle riflessioni nel tempo sviluppate dalla dottrina con riguardo alla natura dei diritti della personalità, è ormai prevalente la soluzione interpretativa che li qualifica come diritti dell'uomo riconosciuti e non creati dall'ordinamento, in quanto preesistenti lo stesso ribadita in F. GALGANO, *Trattato di diritto civile*, Vol. I, III ed., Cedam, Padova, 2014, 171ss. Più specificatamente, se si adotta la prospettiva per cui la tutela del dato personale è intimamente connessa al principio di dignità di cui all'articolo 1 Carta di Nizza, quest'ultimo deve cionondimeno entrare in una necessaria prospettiva di bilanciamento con la libertà d'impresa e con il diritto di proprietà tutelati, rispettivamente, dagli articoli 16 e 17 della Carta medesima. Così G. ALPA, *La "proprietà" dei dati personali*, cit., 15-16.

[41] Cfr. S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, Editori Laterza, 2014, 31-32.

relazionale che, non solo non vieta, ma presuppone l'ingresso di altri nella propria sfera personale.

Già all'indomani dell'adozione della previgente legge n.675/1996, infatti, si notava come la stessa istituzione di un'autorità indipendente denotasse la creazione di un vero e proprio mercato in cui il dato personale "diventa oggetto istituzionale di attività professionalmente organizzata di elaborazione […]. [Una] "risorsa di base", attraverso la quale creare altre informazioni, che a loro volta diventano fattori di produzione potenzialmente utilizzabili a servizio di strategie politiche e imprenditoriali la cui dimensione non ha, altrettanto potenzialmente, alcun limite di base"[42].

Il diritto alla protezione dei dati personali, in quest'ottica, non nasce in contrapposizione alla dimensione economica della circolazione dato, ma come strumento normativo attraverso il quale restituire al soggetto interessato, divenuto "fornitore istituzionale di informazioni", una forma di controllo sulle stesse[43].

In prospettiva analoga si colloca quella dottrina che, ricostruendo il divieto di commercializzazione del corpo umano di cui all'articolo 3 della Carta di Nizza in termini di inalienabilità a titolo oneroso e non di assoluta indisponibilità, vede nel suo mancato richiamo con riferimento agli altri attributi della persona, inclusi i dati personali di cui all'articolo 8, l'apertura di una breccia, poi colta dal legislatore eurounitario, per l'istituzionalizzazione della commercializzazione di elementi costitutivi dell'identità personale[44]. Ne consegue che, ove letto alla luce del mancato espresso recepimento del

[42] C. CAMARDI, Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/1996, 4, *Europa e diritto privato*, 1998, 1049, 1057, rievocando l'analogo scenario paventato da S. RODOTÀ, *Tecnologie e diritti*, Bologna, Il Mulino, 1995, 41ss.

[43] Così C. CAMARDI, Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/1996, cit., 1058 ove sottolinea come "[a]bitudini, gusti, tendendenze, opinioni, credenze religiose e convinzioni politiche, e quant'altro più intimamente contraddistingue la personalità dei cittadini sotto ogni profilo, diventano materiale facilmente reperibile e suscettibile di essere connesso, manipolato, elaborato, trasformato e restituito in una forma che non è più quella originaria, ma è un'altra "cosa", un altro prodotto, dotato di un valore enormemente maggiore, in quanto utile ad essere sfruttato nell'ambito di strategie politiche, elettorali, di opinione, o di pubblicità o di marketing, quali richieste dall'imperativo categorico dell'innovazione permanente che comanda, oggi, il ciclo produttivo delle imprese".

[44] G. RESTA, La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della carta dei diritti), cit., 811 e 815-818. In senso analogo, nel discutere della qualificazione giuridica della personalità, già si era espresso Zeno-Zencovich mettendo in evidenza come "negli ultimi anni si sia evidenziata con sempre maggiore nettezza accanto al tradizionale interesse (morale) all'inviolata personalità, una dimensione economica, patrimoniale della stessa per la quale i tradizionali e consolidati canoni definitori non appaiono del tutto adeguati". V. ZENO-ZENCOVICH, Cosa (voce), *cit.*, § 15. Da notare, tuttavia, come, a dispetto delle menzionate premesse, L'Autore ha poi assunto posizioni tendenzialmente critiche verso la c.d. teoria delle obbligazioni circa la natura giuridica degli "atti" di disposizione degli attributi della personalità nella misura in cui "presuppone [come] già compiuta la qualificazione degli

principio di extrapatrimonialità, e inquadrato nell'ottica della c.d. tutela dalla commercializzazione, il diritto fondamentale *al controllo* dei dati[45] diventa "strumento di garanzia dell'autonomia [dei soggetti interessati] […] rispetto alle logiche pervasive dell'economia"[46], ma non di esclusione delle stesse.

Interiorizzata così la componente mercantilista all'interno della sfera valoriale salvaguardata dal diritto alla protezione dei dati personali, non può non condividersi la posizione di chi, già con riferimento al previgente quadro normativo, notava come "più che una legge a tutela della privacy, la l.n. 675 si atteggia come un vero e proprio sottosistema legislativo volto a regolare ed a legittimare l'attività dei soggetti che professionalmente svolgono attività di raccolta ed elaborazione di dati personali"[47].

Di qui la necessità di focalizzare l'attenzione, dapprima in prospettiva empirica e poi giuridica, sulla posizione del titolare del trattamento non soltanto in quanto portatore di situazioni giuridiche soggettive passive speculari ai diritti e facoltà del soggetto interessato, ma anche e soprattutto in quanto titolare di un'autonoma situazione giuridica soggettiva attiva da alcuni definita "diritto" al trattamento dei dati personali e sulla cui qualificazione giuridica si ritornerà meglio in seguito[48].

Prima di entrare nel dettaglio delle tesi sviluppate con riferimento agli atti di "disposizione" degli attributi della personalità, in generale, e con riferimento alle facoltà di godimento e utilizzazione trasmesse o create in capo al titolare del trattamento, in particolare, è necessario operare una breve ricognizione empirica dei principali "modelli di monetizzazione dei dati" caratterizzanti l'attuale assetto del mercato digitale.

In tale contesto, un ruolo fondamentale –come si anticipava nel precedente paragrafo- è senz'altro rivestito dai *data brokers* (o intermediari informativi). Tale figura professionale è tutt'altro che recente: nata negli anni Sessanta del secolo scorso, è

interessi di cui si dispone." Tema, questo, sul quale si tornerà meglio in seguito. ID., I negozi sugli attributi della personalità, *Diritto dell'informazione e dell'informatica*, 3, 1993, 545, 593.

[45] Cfr. S. RODOTÀ, Tra diritto e società. Informazioni genetiche e tecniche di tutela, 18, *Riv. crit. Dir. priv*., 4, 2000, 571, 588.

[46] G. RESTA, La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della carta dei diritti), cit., 805, spec. nt. 11 ove richiama le teorizzazioni di DIETER GRIMM.

[47] C. CAMARDI, Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/1996, cit., 1062.

[48] Cfr. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., *passim*; D. FARACE, Le persone autorizzate al trattamento dei dati personali, *Rivista Trimestrale di Diritto e Procedura Civile*, 2, 2021, 423 ss.

costituita da un complesso di modelli imprenditoriali altamente variegato, ma genericamente associati allo svolgimento di un'attività professionale consistente nella raccolta, analisi e distribuzione di dati personali. I modelli di c.d. "*personal data economy*" vengono generalmente suddivisi in modelli di c.d. *data-insights* e *data-transfer*, entrambi riconducibili allo schema classico dell'attività di intermediazione[49] e consistenti nell'offrire agli utenti piattaforme in cui, rispettivamente, raccogliere e controllare il processo di circolazione dei propri dati personali, gestendo in modo intuitivo le richieste di accesso da parte delle varie applicazioni e servizi[50], ovvero mettere all'asta i propri dati personali attraverso meccanismi di inclusione diretta nel circuito di distribuzione delle ricchezze generate dai propri dati personali[51].

Paradossalmente, tuttavia, le più tradizionali (e remunerative) forme di *data brokering* non implicano una relazione tra intermediario e soggetto interessato per la gestione dei propri dati (c.d. modello *user-centric*)[52], ma una relazione esterna a cui quest'ultimo rimane estraneo poiché intrattenuta principalmente tra imprese terze interessate ad acquistare le informazioni gratuitamente generate dagli interessati per finalità di marketing. È questo il caso, ad esempio, di Acxiom, azienda leader nel settore del c.d. *database marketing* con una delle più ricche banche dati commerciali al mondo (peraltro attualmente integrata nella piattaforma Cloud offerta da Amazon Web Services)[53]. Alla macrocategoria di *data brokers* possono essere ricondotti anche i gestori

[49] Tale forma di *data brokering*, peraltro, richiama l'attività svolta da quelle *trusted third parties* o *"infomediaries"* che parte della dottrina, circa un ventennio fa, già teorizzava come possibile soluzione alla problematica inerzia mostrata dai soggetti interessati rispetto al regime di trattamento dei loro dati personali, così come predefinito dal titolare del trattamento. P.M. SCHWARTZ, Privacy and Democracy in Cyberspace, 52, *Vand. L. Rev*., 1999, 1609, 1685. Il termine *infomediary* venne coniato da J. HAGEL III, J.F. RAYPORT, The Coming Battle for Customer Information, *Harv. Bus. Rev*., 1997, 53, 54 le cui teorizzazioni sono state poi richiamate da P.M. SCHWARTZ, Internet Privacy and the State, 32, *Connecticut Law Review*, 3, 2000, 815, 841.

[50] Ne sono esempi i servizi offerti da Digi.me (*www.digi.me*), Meeco (*www.meeco.me*) e Cozy Cloud (*www.cozy.io*).

[51] Questo, invece, il servizio (ora sospeso) offerto da Datacoup (*www.datacoup.com*).

[52] V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 51.

[53] Più in generale, come già chiarito in dottrina, "[*g*]*eneral marketing data brokers provide PII and Non PII data for both offline and digital marketing purposes. They license a list of individuals who meet certain criteria to a marketer, a process known as "list rental," or they append specified data elements to a marketer's customer list, a process known as "enhancement." These data brokers aggregate and provide data on individuals and households identifying information (e.g., name, address, phone, and email), demographic information (e.g., age or date of birth, education, and ethnicity), household characteristics (e.g., identifying and demographic information on the spouse, how many children there are and their approximate ages, and how many people live in the house), general financial information (e.g., modeled ranges of estimated household income and modeled estimated net worth), interests (e.g., like to cook, read, water ski, travel abroad, or redecorate the house), lifestyle (e.g., types of cars, and information about*

di cc.dd. "*people search sites o engines*" quali LinkedIn, spokeo.com e peoplefinders.com specializzati nella raccolta di profili professionali accessibili, ad esempio, a datori di lavoro in cerca di personale o, all'inverso, a potenziali clienti in cerca di prestatori di determinati servizi o professionalità[54]. Ancora, l'attività di *data brokering* può declinarsi in attività di aggregazione e riorganizzazione di specifiche tipologie di informazioni pubblicamente accessibili e, in questo settore, tra i principali attori è possibile annoverare Experian. Quest'ultima, peraltro, può essere anche qualificata come una agenzia di "*consumer reporting*" (c.d. *Credit Reporting Agency* o CRA), più genericamente riconducibile alla categoria di *credit bureaus* deputate allo svolgimento di una attività di raccolta e analisi di informazioni che si contraddistingue per la strumentalità all'assunzione di decisioni in ambiti altamente sensibili quali la ricerca e la selezione di personale e la valutazione del merito creditizio della clientela[55] e sulle quali si ritornerà più approfonditamente in seguito[56].

È proprio questa peculiare declinazione assunta dal fenomeno del *data brokering*, infatti, ad assumere maggiore rilievo ai fini dell'analisi che verrà svolta nei prossimi capitoli, in quanto fonte di complessi problemi di coordinamento tra le esigenze imprenditoriali sottese a tale diffuso modello di business e i diritti di accesso degli interessati che vedono incisa la propria sfera giuridica per effetto dei processi decisionali automatizzati per tal via condotti.

Prima di passare all'analisi di tale disciplina, tuttavia, rimane un ultimo passaggio interpretativo preliminare: chiarire la natura giuridica del rapporto che si viene ad instaurare tra titolare del trattamento e soggetto interessato per effetto del verificarsi di una delle basi giuridiche di cui agli articoli 6 e 9 GDPR. In particolare, preso atto della necessità di superare, perlomeno con riferimento alla peculiare figura del dato personale, la rigida distinzione fra categorie dell'essere e dell'avere, si procederà all'inquadramento dogmatico della situazione giuridica soggettiva attiva configurabile in capo al titolare del trattamento avente ad oggetto quel bene intangibile, dato personale, giuridicamente

property owned, such as price, value, size, age, features, and mortgage company), and major life events (e.g., recently got married, divorced, had a child, or bought a new house)." J. BARRETT GLASGOW, *Data Brokers: Should They Be Reviled or Revered?*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2018, 31.

[54] Per maggiori riflessioni sulle implicazioni giuridiche in punto di protezione dei dati personali derivanti da tale tipologia di intermediazione informativa si veda meglio *infra sub* Cap. III, §3.6.

[55] J. BARRETT GLASGOW, *Data Brokers: Should They Be Reviled or Revered?, cit.*, 28.

[56] Vedi infra Cap.III.

rilevante non solo in quanto mera espressione della personalità dell'interessato, ma anche in quanto fonte degli interessi economici sottesi al suo sfruttamento ed oggetto di un'attività imprenditoriale altamente remunerativa.

1.3. Il "diritto" al trattamento dei dati personali

L'intrinseca dicotomia messa in evidenza nei precedenti paragrafi, consentendo di guardare alla disciplina dettata dal GDPR da una prospettiva ermeneutica assiologicamente neutrale, induce l'interprete a prestare maggiore attenzione al chiaro, ma a lungo trascurato, manifesto programmatico racchiuso nei primi considerando del Regolamento. Quest'ultimo, infatti, apre il suo lungo e complesso dettato normativo mettendo in chiaro come l'obiettivo perseguito, al pari del mandato legislativo conferito al Parlamento europeo e al Consiglio dall'articolo 16 par.2 TFUE[57], sia duplice: "armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati *e* assicurare la libera circolazione dei dati personali tra Stati membri"[58].

Peraltro, offrendone anche un criterio di ordinazione prioritaria, il legislatore eurounitario ha puntualizzato come, seppure sempre nel rispetto di tutti i diritti fondamentali, fra cui, in particolare, quello alla protezione dei dati personali[59], "[p]er il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati

[57] "L'articolo 16, paragrafo 2, TFUE conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati" così recita il Considerando 12 del Reg. (UE) 2016/679, rievocando il dettato dell'articolo 16 par. 2 TFUE per cui "[i]l Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti". In senso analogo v. anche l'articolo 39 TUE per cui "[c]onformemente all'articolo 16 del trattato sul funzionamento dell'Unione europea e in deroga al paragrafo 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, *e le norme relative alla libera circolazione di tali dati*". Corsivo aggiunto.

[58] Corsivo aggiunto. Reg. (UE) 2016/679, Considerando 3.

[59] GDPR, Considerando 4.

personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali"[60].

Ne consegue che, non solo il rafforzamento del mercato dei dati rientra a pieno titolo fra gli interessi a cui il Regolamento attribuisce rilevanza giuridica, ma risulta anche espressamente sovraordinato, seppure non in modo assoluto, all'esigenza di protezione dei dati degli interessati[61]. Tale osservazione traghetta l'interprete verso la preliminare conclusione per cui se è vero che il diritto alla protezione dei dati personali ha ad oggetto questi ultimi, sebbene in via mediata, in quanto riflesso del diverso interesse alla salvaguardia dell'identità personale degli interessati; è altrettanto innegabile che, accanto a quest'ultimo, sia configurabile una diversa situazione giuridica soggettiva attiva in capo al titolare del trattamento avente ad oggetto la medesima risorsa informativa rappresentata dal dato, ma in quanto "bene intangibile" la cui rilevanza giuridica non è collegata ad un aspetto della personalità ma ad esigenze di mercato di natura squisitamente economico/patrimoniale: il "diritto" al trattamento dei dati personali[62].

Al di là delle disposizioni a contenuto programmatico sin qui richiamate, parte della dottrina ha radicato il riconoscimento implicito della "facoltà" di trattare i dati altrui nel dettato dell'articolo 8 par.2 della Carta di Nizza, nella parte in cui, imponendo il rispetto del principio di lealtà e limitazione delle finalità, "presuppo[ne] implicitamente – nel settore del diritto alla libertà di iniziativa economica[…]- anche il riconoscimento del complementare "diritto" a trattare dati personali altrui, allorché il trattamento sia basato su un fondamento legittimo e sia conforme ai principi di lealtà e di finalità [63]."

[60] GDPR, Considerando 13.

[61] Sulla caduta del richiamo alla dignità operato dalla previgente normativa si veda quanto osservato da C. IRTI, Dato personale, dato anonimo e crisi del modello normativo dell'identità, cit., 381, spec. nt. 12, ove richiama il dibattito sull'emersione di una prospettiva "patrimonialistica" nel regime di circolazione del dato personale già intuita da S. SIMITIS, Il contesto giuridico e politico della tutela della privacy, *Riv. crit. dir. priv*., 4, 1997, 575 ss.

[62] In senso affine BRAVO, notando come, sebbene nell'impianto normativo in esame non scompaia la dimensione di tutela della persona, il GDPR innova la disciplina previgente attraverso un "approccio volto ad enfatizzare maggiormente la dimensione della libera circolazione rispetto a quello teso ad esaltare la dimensione di tutela della persona rispetto al trattamento dei dati personali", inquadrando tali due dimensioni in un rapporto di bilanciamento e non di reciproca esclusione. ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 12. Cfr. M. ARE, voce Beni immateriali, *cit*., § 6, specialmente nella parte in cui sottolinea come "comunque si voglia considerare la natura giuridica della tutela della personalità, è da tener separata la protezione di questa dal diritto patrimoniale sul bene immateriale."

[63] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 56.

In quest'ottica, le basi giuridiche dettate dagli articoli 6 e 9 GDPR assumono la valenza di condizioni costitutive di tale diverso "diritto" del titolare del trattamento, il quale, per effetto del venire ad esistenza di uno di tali circostanze/presupposti, vede conferita rilevanza giuridica alla sua posizione di interesse allo sfruttamento del potenziale economico del dato personale[64]. Assumendo una prospettiva ermeneutica teleologicamente orientata alla definizione della posizione giuridica del titolare del trattamento, quindi, le basi giuridiche diverse dal consenso acquistano rilevanza centrale nella misura in cui, sottraendo dalla sfera di disponibilità dell'interessato i trattamenti sulle stesse fondati[65], definiscono i contorni delle prerogative del titolare sul dato personale altrui.

In altri termini, approcciato da tale angolo prospettico, il diritto alla protezione dei dati degrada a (co-)formante[66] assiologico della disciplina contenuta nel GDPR. Quest'ultima, infatti, preso atto della posizione di controllo sui propri dati che il primo fissa in capo all'interessato, vi costruisce attorno un'infrastruttura legislativa di pesi e contrappesi avente il principale obiettivo di conferire un sufficiente spazio di libertà al

[64] In senso analogo, la dottrina richiamata osserva come "sotto il profilo strutturale, le "condizioni di liceità" oper[ino] come elementi indefettibili della fattispecie di trattamento e al contempo, […] elementi strutturali e fondamentali per la configurabilità del diritto a trattare dati personali altrui, operanti come meccanismi di valutazione in ordine sia alla meritevolezza degli interessi perseguiti con il trattamento, sia al bilanciamento degli interessi, dei diritti e delle libertà "fondamentali" facenti capo al titolare ed all'interessato." F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 87. Cfr. T. ASCARELLI, *Teoria della concorrenza e dei beni immateriali*, III ed., Milano, Giuffré, 1960, 299ss, ove si osserva come, se nel caso delle cose materiali è sufficiente una norma che identifichi la fattispecie costitutiva del diritto, per le creazioni intellettuali è invece necessaria una disciplina normativa della fattispecie costitutiva del bene.

[65] Nelle parole di ZENO ZENCOVICH: "si potrebbe ritenere che siano sottratti alla disponibilità del titolare quelle utilizzazioni (il termine è inteso in senso lato e atecnico) di aspetti della personalità che terzi possono lecitamente compiere anche senza il suo consenso". ID., Profili negoziali degli attributi della personalità, cit., 548.

[66] Come confermato dal Considerando 4 del GDPR ai sensi del quale "[i]l presente regolamento rispetta *tutti* i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, *in particolare* il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica" (corsivo aggiunto). Interessante, al riguardo, l'angolo prospettico assunto da BRAVO nell'osservare come il trattamento dei dati personali "sia il "fatto giuridico" che costituisce il presupposto per l'accesso alla tutela della protezione dei dati personali" chiarendo poi come "[l]e esigenze di tutela dell'interessato, in altre parole, sorg[ano] dal momento in cui viene posto in essere un "trattamento" dei propri dati personali", facendo così propria la menzionata logica di internalizzazione della dimensione mercantilista della circolazione del dato personale all'interno del diritto fondamentale alla sua protezione. Così F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 52.

fenomeno del trattamento dei dati personali altrui, in quanto strumentale al rafforzamento del mercato interno[67].

L'obiettivo dei seguenti paragrafi, quindi, è quello di rileggere i tradizionali sforzi ermeneutici di inquadramento della fattispecie senza arrivare ad attribuire al dato personale valore di pura merce[68], ma senza nemmeno dover necessariamente cadere nella trappola interpretativa delle "forme di utilizzazione della personalità" che hanno reso notoriamente complesso definire il contenuto degli atti autorizzativi degli stessi[69]. Riprendendo, allo scopo, la classificazione operata quasi un trentennio fa da Zeno-Zencovich[70], il capitolo proseguirà ripercorrendo i tratti salienti del dibattito dottrinale sfociato nella tesi "realista" dei diritti dominicali sul dato, nella tesi "industrialista" della proprietà intellettuale sul dato e nella tesi "obbligatoria" del dato come oggetto di un rapporto sinallagmatico a carattere patrimoniale, vagliandone però l'attitudine a definire la natura del diritto insorgente in capo al titolare del trattamento e non del soggetto interessato[71].

[67] In senso affine, assimilava il diritto alla protezione dei dati personali ad una "precondizione" per il pieno godimento degli altri diritti fondamentali S. RODOTÀ, Tra diritti fondamentali ed elasticità della normativa. Il nuovo codice sulla privacy, *Europa e diritto privato*, 1, 2004, 1, 3.

[68] Sul rifiuto di tale impostazione dogmatica da parte delle Istituzioni europee si veda *infra sub* §1.6 e *sub* Cap. II, § 2.6 in punto di disciplina sulla fornitura di servizi digitali.

[69] "Si privilegia, insomma, sulla scia di una risalente distinzione, l'inquadramento della personalità fra le categorie dell'essere e non dell'avere. Ciò tende a favorire soprattutto forme di tutela del diritto da interventi esterni che alterino in senso negativo lo status quo: in primo luogo il principio generale della responsabilità civile per fatto illecito. Mentre invece si rende problematica la disciplina giuridica delle forme di utilizzazione della personalità quale oggetto di rapporti patrimoniali nei quali occorre, necessariamente, scindere gli aspetti di immediata e diffusa rilevanza economica (il nome, l'immagine) da altri più tradizionalmente non patrimoniali (l'onore, la riservatezza). Si spiegano così molte delle difficoltà che incontra l'interprete quando voglia chiarire l'esatto contenuto degli atti giuridici autorizzativi dell'uso di attributi personali di un altro soggetto, sia per quanto riguarda l'ampiezza del consenso, sia per quanto riguarda la sua revocabilità, o, comunque, modificabilità unilaterale". V. ZENO-ZENCOVICH, Cosa (voce), *cit.*, § 15.

[70] V. ZENO-ZENCOVICH, Profili negoziali degli attributi della personalità, cit., 593-597.

[71] Come condivisibilmente notato in dottrina, infatti, "l'insistenza normativa per gli obblighi e per i divieti del titolare del trattamento finisce per determinare, anche culturalmente, una fuorviante interpretazione della disciplina sulla protezione e libera circolazione dei dati, che porta a sottovalutare le prerogative del titolare del trattamento". F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 68.

1.4. La proprietà dato personale nel quadro del neo-realismo informativo

Le premesse dogmatiche sin qui compiute consentono di reinterpretare le riflessioni dottrinarie postulanti prerogative di matrice dominicale sul dato personale assumendo il punto di vista del titolare del trattamento. In particolare, muovendo dall'impostazione ermeneutica per cui il "dato costituisce l'oggettivazione della personalità del soggetto"[72] e il consenso integra gli estremi di "una condizione soggettiva per la reificazione dei dati personali" rendendoli "beni suscettibili di autonoma considerazione economica"[73], è possibile giungere alla preliminare conclusione per cui, ragionando in via analogica, le altre basi giuridiche di cui agli artt. 6 e 9 GDPR non possono che assurgere a condizioni *oggettive* destinate a produrre il medesimo effetto di reificazione del dato personale[74].

Ne consegue che, il trattamento lecito disciplinato dal Regolamento verte sempre su dati personali che, seppure non assimilabili a pura merce di scambio in ragione del loro legame personalistico con l'identità del soggetto interessato[75], rilevano in sé, in quanto istantanea cristallizzazione di un frammento d'identità temporalmente circoscritto e per questo altro rispetto alla persona che lo ha fornito.

Solo in quest'ottica è possibile comprendere la prospettiva ermeneutica assunta da quella recente dottrina che, riprendendo gli approcci dominicali al rapporto dato-soggetto interessato nati in contesti di *common law*, promuove il superamento del retaggio dottrinale della non commerciabilità del dato personale per effetto dell'importazione di

[72] V. ZENO-ZENCOVICH, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffré, 1999, 168.

[73] V. CUFFARO, *A proposito del ruolo del consenso*, ivi, 121.

[74] In senso soltanto parzialmente analogo si è espressa anche la dottrina che vede nelle condizioni di liceità "il presupposto necessario non solo per la liceità del trattamento, ma anche per la configurazione stessa del "diritto a trattare dati personali altrui". L'Autore, tuttavia, muove da una nozione di diritto al trattamento del dato altrui avente ad oggetto le mere operazioni operazioni, economicamente e patrimonialmente rilevanti, su dati personali e non le informazioni per tal via ottenute come, invece, in tale sede si sostiene e di cui si dirà meglio *infra* nel testo.F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 75.

[75] Sulla funzione "monetaria" (rectius di mezzo di scambio) del dato personale si dirà meglio a breve *infra sub* §1.6 spec. nt. 178, nonché *sub* Cap. II, §2.6.

un modello nordamericano di "proprietà" sul proprio patrimonio informativo, in quanto più coerente alla mercificazione *de facto* subita dallo stesso nel contesto *Big Data*[76].

Sulle profonde affinità genetiche che hanno storicamente legato lo sviluppo della nozione statunitense di privacy ad una accezione lockiana di proprietà, così come sul recente *revirement* filo-continentale registrato in California, si ritornerà più approfonditamente in seguito[77], tuttavia, è sin d'ora importante notare come tale matrice dominicale, spontaneamente emersa da un sostrato culturale tradizionalmente ostile ad ingerenze esterne (specialmente se governative) nella sfera privata dei cittadini[78], ha trovato terreno fertile nella mancata adozione di un chiaro modello assiologico, prima ancora che giuridico, di disciplina degli interessi pubblici e privati coinvolti nell'economia dei dati[79]. L'inerzia del legislatore statunitense, quindi, ha giustificato e

[76] A A. BOERDING, N. CULIK, C. DOEPKE, T. HOEREN, T. JUELICHER, C. ROETTGEN, M.V. SCHOENFELD, Data Ownership. A Property Rights Approach from a European Perspective, cit., 325 e 331ss.. In particolare, gli Autori supportano la propria tesi argomentando di un asserito rafforzamento della posizione di controllo dell'interessato sui propri dati realizzata per effetto dell'introduzione, ad opera del GDPR, degli istituti della portabilità dei dati (sul quale si ritornerà più approfonditamente a breve nel testo) e del diritto all'oblio. Quanto a quest'ultimo argomento, basti qui osservare che se lo *ius excludendi alios*, in quanto estrinsecazione di un diritto assoluto, può essere esercitata verso chiunque, l'interessato ha diritto di ottenere la cancellazione dei propri dati soltanto "dal titolare del trattamento". Per il caso in cui quest'ultimo abbia condiviso tali dati con altri titolari del trattamento, infatti, non soltanto il legislatore eurounitario si è limitato a porre in capo al primo il più limitato obbligo di informare "[gli altri] titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali", ma ha anche temperato tale previsione vincolandola ad un canone di ragionevolezza parametrato alla tecnologia disponibile e ai costi di attuazione delle misure allo scopo necessarie (Articolo 17, para 2 GDPR). Peraltro, a riprova della marcata funzione sociale del dato personale, il diritto all'oblio è soggetto ad ampie deroghe, tutte riconducibili a prevalenti interessi della collettività, quali il diritto alla libertà di espressione ed informazione, l'adempimento di un obbligo legale, lo svolgimento di un compito di pubblico interesse, l'esercizio di pubblici poteri, il soddisfacimento di interessi pubblici nel settore della sanità pubblica, l'esercizio del diritto di difesa in sede giudiziaria o, ancora, l'archiviazione nel pubblico interesse (Articolo 17 para 3 GDPR). In senso analogo si è espresso anche J.M. VICTOR, The Eu General Data Protection regulation: Toward a Property Regime for Protecting Data Privacy, *Yale Law Journal*, 2013, 515, 518-519. Sul concetto di c.d. proprietà di fatto sul dato si veda N. PURTOVA, The Illusion of Personal Data as No One's Property, 7, *Law, Innovation and Technology*, 1, 2015, 83ss. Cfr. E.J. JANGER, Privacy, Property, Information Costs, and the Anticommons, *Hastings L.J*., 54, 2003, 899, 913-918; L. LESSING, The Architecture of Privacy, 1, *Vand. J. Ent. L. & Prac*., 1999, 56, 63; R.S. MURPHY, Property Rights in Personal Information: An Economic Defense of Privacy, 84, *Geo. L.J*., 1996, 2381ss; V. JANEČEK, Ownership of Personal Data in the Internet of Things, 34, *Computer L. & Security Rev*., 5, 1039ss.

[77] V. *infra sub* Cap. III, § 3.9.

[78] V. *infra sub* Cap. III, § 3.2.

[79] Emblematiche, in questo senso, le parole di Pamela Samuelson, secondo la quale "[*m*]*yriad reasons explain why the U.S. response to the challenges of information privacy for an information society has been so much slower, more erratic, and less comprehensive than in the E.U. Among them are certainly considerable differences in the regulatory cultures of the U.S. and the E.U., as well as dissimilar attitudes toward the private sector and toward technology. However, a serious impediment to a comprehensive approach in the U.S. is the lack of clarity in this country about the nature of the interest that individuals have in information about themselves: Is it a commodity interest, a consumer protection interest,a personal dignity interest, a civil right interest, all of the above, or no interest at all? 238 One of the strengths of the EU Directive is that the regulatory regime it embodies is consistent with its underlying conception of*

reso giuridicamente sostenibili approcci proprietari che, per quanto astrattamente più adeguati al valore di mercato assunto dal dato personale, nell'ordinamento eurounitario non possono che infrangersi contro il granitico scoglio normativo e dogmatico della natura fondamentale e personalistica del diritto alla protezione dei dati personali[80].

Se, tuttavia, riprendendo le fila del ragionamento sin qui proposto, si guarda al dato personale come cristallizzazione obiettivizzata del frammento d'identità in esso rappresentato, e quindi come entità pregiuridica immateriale reificata e autonomamente suscettibile di formare oggetto del diverso interesse giuridicamente rilevante al suo trattamento sorto in capo al titolare per effetto del verificarsi di una delle condizioni di liceità di cui agli artt. 6 e 9 GDPR, è possibile offrire un nuovo angolo prospettico da cui osservare tali sforzi interpretativi.

A tal riguardo, recente dottrina, facendo propria un'accezione c.d. strutturale della nozione di diritto fondamentale[81], ha osservato come, in quanto elemento costitutivo di una delle priorità effettive espressamente perseguite dall'ordinamento eurounitario[82], il "diritto" al trattamento dei dati altrui sia astrattamente suscettibile di integrare gli estremi di un diritto fondamentale di libertà, al pari delle altre libertà economiche, prima fra tutte la libertà d'impresa *ex* art. 16 della Carta dei diritti fondamentali dell'Unione europea[83].

---

information privacy as a fundamental human right. Without a coherent conception about the nature of a person's interest in personal data, it is difficult to design a legal regime to protect this interest appropriately". ID., Privacy as Intellectual Property, 52, *Stan. L. Rev*., 2000, 1125, 1170-1171.

[80] Cfr. S. PATTI, *Consenso, sub art. 23*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, t. I, Padova, Cedam, 2007, 541ss; G. RESTA, V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, cit., *passim*; A. MANTELERO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, Giuffré, 2007; V. MAYER-SHÖNBERGER, Beyond Privacy, Beyond Right. Toward a 'System' Theory of Information Governance, 98, *Cal. L. Rev*., 2010, 1853ss.

[81] In particolare, l'Autore, fa notare come l'ordinamento eurounitario abbia adottato un'accezione strutturale di diritto fondamentale, riferita all'Unione stessa. In altri termini, la nozione di diritto fondamentale fatta propria, ad esempio, nella Carta di Nizza, guarda ai diritti fondamentali come a diritti fondanti l'ordinamento sovranazionazionale, implicitamente rigettando così l'impostazione formale autorevolmente avanzata da FERRAJOLI (e tipica delle esperienze giuridiche nazionali) per cui i diritti fondamentali afferiscono alla persona in quanto diritti soggettivi propri di ogni essere umano in quanto tale. Così F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 62-63 richiamando L. FERRAJOLI, *Diritti fondamentali. Un dibattito teorico*, Roma, Editori Laterza, 2001, 5 e P. COSTA, Diritti fondamentali (storia dei) (voce), *Enc. dir.*, II, Milano, Giuffré, 2008, 365ss.

[82] Come reso evidente dai numerosi manifesti programmatici pubblicati dalle istituzioni europee in punto di promozione del Mercato Unico Digitale, prima, e dell'Economia dei dati, ora con la COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia europea per i dati* (Bruxelles, 19 febbraio 2020) (COM(2020) 66 final).

[83] Nelle parole dell'Autore: "[l]a natura di tale diritto è dunque, nella prospettiva ordinamentale eurounitaria, quella di un diritto "fondamentale", di matrice principalmente (ma non esclusivamente) economica, che è partecipe della (componente privatistica) più ampia libertà di circolazione dei dati e che

Tale conclusione, peraltro, non sarebbe contraddetta neppure dal carattere indubbiamente relativo del "diritto" al trattamento, fortemente limitato dai pervasivi diritti di accesso e cancellazione degli interessati, in quanto, come da tempo chiarito dalla Corte di Giustizia, i diritti fondamentali, riguardati alla luce della loro funzione sociale, non sono esenti da bilanciamento, cioè da restrizioni strumentali alla realizzazione di confliggenti obbiettivi di pubblico interesse[84].

In quest'ottica, quindi, e parzialmente contraddicendo le conclusioni raggiunte dalla dottrina richiamata[85], il GDPR assurge sì a c.d. legge di collisione, ma recante una disciplina che, seppure formulata dalla prospettiva del soggetto interessato, ha ad oggetto la definizione del contenuto e dei confini del diritto al trattamento dei dati personali altrui, ponendovi restrizioni idonee, necessarie e proporzionate al rispetto del confliggente diritto alla protezione dei dati personali che, perciò, assume rilievo centrale ma soltanto in negativo, definendo i confini entro i quali contenere le contrapposte libertà contenuto della situazione giuridica soggettiva attiva facente capo al titolare.

presenta un collegamento funzionale sia con la realizzazione del mercato europeo, che -proprio attraverso la circolazione dei dati- trova attuazione. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 67.

[84] Così Corte di Giustizia dell'allora Comunità Economica Europea, sentenza del 13 luglio 1989, causa C-5/88, *H. Wachauf c. Repubblica federale di Germania*, EU:C:1989:321, par. 18 richiamata da F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 164, spec. nt. 44. Cfr. A. RICCI, Sulla "funzione sociale" del diritto alla protezione dei dati personali, 33, *Contratto e impresa*, 2, 2017, 586, *passim*.

[85] Le riflessioni qui condotte, infatti, muovono dall'assunto opposto a quello fatto proprio da BRAVO per cui "il diritto alla protezione dei propri dati personali, non è in rapporto di necessaria contrapposizione" con il diritto al trattamento dei dati altrui e quest'ultimo "può essere anzi funzionalmente collegato con il diritto alla protezione dei dati personali ed essere strumentalmente indirizzato al soddisfacimento dell'interesse del soggetto a cui i dati personali si riferiscono: non c'è contrapposizione antagonista, ad esempio, tra titolare del trattamento e interessato quando il trattamento sia necessario per esigenze di cura o per tutelare un diritto in sede giudiziaria, ovvero per eseguire le prestazioni contrattuali di diversa natura richieste dall'interessato medesimo (es.: servizi di trasporto, bancari, fornitura delle utenze, compravendita di beni, corrispondenza postale o telematica, etc.). ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 66. Nella prospettiva qui fatta propria, invece, dire che il trattamento possa operare anche a vantaggio del soggetto interessato, rispondendo ad altri suoi interessi, non significa negare che le operazioni di trattamento e gli interessi perseguiti dal titolare siano in ontologica contrapposizione agli interessi che l'ordinamento eurounitario ha inteso salvaguardare con il riconoscimento del diritto alla protezione dei dati personali. Tutte le prerogative che il GDPR riconosce al soggetto interessato, infatti, si traducono in limiti o doveri posti in capo al titolare del trattamento, e sebbene sia assolutamente condiviso e anzi posto a premessa iniziale e impostazione di fondo dell'intero capitolo l'assunto per cui "l'insistenza normativa per gli obblighi e per i divieti del titolare del trattamento finisce per determinare, anche culturalmente, una fuorviante interpretazione della disciplina sulla protezione e libera circolazione dei dati, che porta a sottovalutare le prerogative del titolare del trattamento" (Ivi, 68), è purtuttavia innegabile l'ontologica conflittualità che si instaura tra il diritto dell'interessato a controllare e limitare la circolazione dei propri dati e il "diritto" del titolare di raccogliere e analizzare tale patrimonio informativo nel modo e per le finalità più ampi possibili.

Quest'ultima, accogliendo l'impostazione ermeneutica richiamata, può perciò essere condivisibilmente qualificata come un diritto soggettivo composto da un complesso di facoltà cc.dd. determinative[86], organizzative[87] e gestionali[88] singolarmente ricavabili dal complessivo disposto normativo del Regolamento ed esercitabili nel rispetto dei limiti ivi fissati, primi fra tutti quelli posti dall'obbligo di rispettare i principi di minimizzazione dei dati, limitazione delle finalità, trasparenza e responsabilizzazione.

Chiariti così i contorni del diritto soggettivo al trattamento dei dati personali altrui accogliendo la tesi della sua natura di diritto di libertà (economica) fondamentale, in quanto strumentale alla realizzazione del mercato unico digitale quale priorità dell'ordinamento eurounitario, ma non necessariamente assoluto e quindi bilanciabile con il (qui ritenuto[89]) confliggente diritto alla protezione dei dati personali, vi è ora da chiedersi se tale complesso di prerogative presenti *de iure condito*, ovvero sia auspicabile conferirvi *de iure condendo*, una declinazione dominicale affine al diritto di proprietà.

Non è, infatti, condivisibile la conclusione raggiunta dalla dottrina sin qui richiamata per cui "il "diritto a trattare dati personali altrui" non ha ad oggetto, in via diretta e immediata, i "dati" personali *ex se* considerati, ma le "*operazioni*" che lecitamente possono essere compiute su tali dati"[90]. Ciò in quanto si accetta

[86] Come, ad esempio, la facoltà di definire le finalità e i mezzi del trattamento di cui all'articolo 4 par.1 n. 7 GDPR. Ivi, 61 e 74.

[87] Come la facoltà di mettere in atto le misure tecniche e organizzative, incluse quelle di pseudonimizzazione e le altre misure di *privacy by design* e *default*, per il perseguimento delle finalità predeterminate e con i mezzi predisposti, ricavabile dall'obbligo del rispetto di uno standard di adeguatezza necessario a garantire e dimostrare il rispetto dei limiti fissati dal GDPR di cui agli articoli 24 e 25 dello stesso. Ivi, 111.

[88] Esemplificato dalla facoltà di designare responsabili e rappresentanti del trattamento ai sensi degli articoli 27 e 28 GDPR, nonché di beneficiare dei vantaggi economici così conseguiti che la dottrina richiamata ricava analogicamente dai diritti esclusivi di utilizzazione economica delle banche dati di cui all'articolo 102 *bis* l.d.a. (Ivi, 74) ma che, nell'impostazione qui assunta, è più semplicemente desumibile dalla mancanza di una prescrizione di senso opposto e quindi dall'assenza di un potenziale conflitto tra la facoltà del titolare di trarre guadagno dall'analisi dei dati lecitamente raccolti e il diritto dell'interessato alla protezione degli stessi.

[89] Sulla diversa posizione sul punto assunta dalla dottrina richiamata si veda meglio *supra sub* Nt. 78.

[90] Così F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 109. Si precisa che sebbene il legislatore europeo nel GDPR abbia fatto riferimento alla titolarità "del trattamento" e non "del dato" (come *de iure condendo* sembra aver fatto, invece, il legislatore del *Data Governance Act*), ciò non si pone in contrasto con l'obiettivo dell'analisi condotta nel capitolo: mettere in luce un percorso di progressiva reificazione dell'informazione inizialmente rappresentata dal dato personale per effetto delle operazioni di trattamento dello stesso. Ciò significa dire, in altri termini, come a più riprese ribadito nel testo, che il titolare del trattamento, a seguito delle operazioni di raccolta e analisi del dato verrà ad ottenere informazioni altre rispetto al singolo dato originariamente raccolto, ma dallo stesso inferite e, almeno in parte, riferibili allo stesso soggetto interessato. Ne consegue che, parlare di titolarità sul metadato non significa porsi in contrasto con una concezione di titolarità del trattamento intesa come inconfigurabilità

quell'impostazione dogmatica per cui il dato personale per effetto del verificarsi di una delle basi giuridiche di cui agli artt. 6 e 9 GDPR subisce un effetto di reificazione che, pur non rendendolo *res* nel senso di *cosa* in senso giuridico già menzionato, lo rende *bene* intangibile (nel senso già descritto) proprio perché oggetto di quello che si era genericamente definito un interesse giuridicamente rilevante al suo trattamento, e che si è ora meglio qualificato come diritto soggettivo nei termini sin qui esposti[91].

Ne consegue che, non essendo possibile escludere *in nuce* una "titolarità" sui dati trattati da parte del titolare del trattamento, è necessario verificare se l'insieme delle menzionate prerogative riconosciute dal GDPR al titolare del trattamento presentino quei caratteri di assolutezza, immediatezza ed esclusività tipizzanti la fattispecie del diritto di proprietà e strutturalmente giustificati dalla materialità della cosa che la tradizione romanistica individua come suo esclusivo oggetto[92].

In questo senso, pur escludendo, per i motivi già espressi, l'indispensabilità del tratto dell'assolutezza, evidentemente assente nel diritto a trattare dati personali altrui, e pur volendo superare (ammesso che sia dogmaticamente possibile) la canonica impostazione romanistica della tipicità dei diritti reali e della materialità della cosa che ne forma oggetto, tralasciando così l'elemento della immediatezza del rapporto con il dato personale, rimane comunque difficilmente configurabile in capo al titolare del

di diritti di proprietà sui singoli dati personali, ma significa porsi in linea di continuità con tale ragionamento e fare un passo ulteriore, ragionando sulle posizioni giuridiche soggettive che si vengono ad incardinare sul metadato quale prodotto del trattamento che, pur partendo dal singolo dato personale, racchiude informazioni diverse e ben più preziose nel contesto del mercato dei dati. V. anche Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla Governance europea dei dati (Atto sulla governance dei dati) (Bruxelles, 25 novembre 2020, COM(2020) 767 final), ove si fa riferimento a concetti di "titolarità sul dato" e "metadato" soltanto parzialmente coincidenti con quelle adottate nel testo. In senso parzialmente contrario, F. BRAVO., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018, *109*.

[91] Al contrario, operando una "iperbolica" assimilazione del dato al corpo umano, l'Autore paragona il titolare del trattamento ad un chirurgo che si accinge ad effettuare un intervento su un paziente con la conseguenza che "il corpo di quest'ultimo non è nella sua disponibilità giuridica, ma egli interviene su di esso legittimamente […] con delle operazioni di trattamento finalizzate a soddisfare, nello svolgimento di tale attività professionale, un interesse del paziente. […] *Mutatis mutandis* [prosegue l'Autore] è quanto avviene con il trattamento di dati personali […] [nella misura in cui] il titolare del trattamento è "legittimato" a porre in essere operazioni sui dati (finché non venga meno, per ciascuno dei dati trattati, la condizione di liceità legittimante il trattamento medesimo), per finalità determinate e ammesse dall'ordinamento -volte a realizzare un interesse del soggetto a cui i dati si riferiscono, di soggetti terzi o dello stesso titolare del trattamento- senza che sia di ostacolo il fatto che dal trattamento il titolare ricavi eventualmente un ritorno economico." Ivi, 109 spec. nt. 116.

[92] Così S. PUGLIATTI, *La proprietà nel nuovo diritto*, 250. Contra S. SATTA, Cose e beni nell'esecuzione forzata, cit., 354.

trattamento una facoltà esclusiva di godimento e disposizione del dato assimilabile a quella di matrice dominicale.

De iure condito, il principale ostacolo ad una tale ricostruzione interpretativa è individuabile nel diritto alla portabilità dei dati di cui all'articolo 20 GDPR. Se, infatti, il diritto di accesso del soggetto interessato *ex* art. 15 GDPR neutralizza sì lo *ius excludendi omne alios* del titolare ma solo rispetto alla singola persona fisica che ha fornito l'informazione, l'obbligo del titolare di non ostacolare e, anzi, ove tecnicamente fattibile, di operare in prima persona la trasmissione dei dati personali di qualsiasi interessato ne abbia fatto richiesta ad una pletora potenzialmente illimitata di altri titolari, rende sensibilmente più contratta la sfera degli *omnes alios* astrattamente escludibili dal godimento dei dati, così come dei dati potenzialmente suscettibili di controllo esclusivo da parte del titolare: limitati a quelli raccolti per effetto di una base giuridica diversa dal consenso dell'interessato ex artt. 6(1)(a) e 9(2)(a) o dall'esecuzione di un contratto *ex* art. 6 (1)(b)[93].

Ne consegue che, pur volendosi aprire a evidenti forzature dogmatiche dell'istituto, la disciplina dettata dal Regolamento rende il dato personale un bene intangibile difficilmente suscettibile di godimento esclusivo[94] e, perciò, più affine a quei beni che, secondo la distinzione di Irti, essendo insuscettibili di formare punto di riferimento di esclusione di terzi, risultano comunque punto di riferimento di un'attività della persona (cc.dd. beni oggetto di uso)[95].

Anche assumendo una prospettiva *de iure condendo*, infatti, sebbene sia noto ed indubbio che la non rivalità economica non precluda una appropriabilità giuridica frutto di chiare scelte legislative[96], non sembra che gli obiettivi programmatici fatti propri dalle

[93] Articolo 20 par. 1 lett. (a) e par. 2.

[94] Pone l'accento sulla suscettibilità del bene di formare oggetto di godimento esclusivo D. MESSINETTI, *Oggettività giuridica delle cose incorporali*, cit., 36.

[95] A tal proposito va ricordata la distinzione tra bene oggetto di uso e, quindi, punto di riferimento di un'attività umana, e il bene oggetto di diritto su cui fa invece perno lo *ius excludendi alios* tratteggiata da N. IRTI, *Proprietà e impresa*, Napoli, Jovene, 1965, 106ss.

[96] Interessanti, al riguardo, le riflessioni di G. PUGLIESE, Dalle «res incorporales» del diritto romano ai beni immateriali di alcuni sistemi giuridici odierni, *Riv. trim. dir. proc. civ*., 1137, 1181 ove osserva come "non esistono cose oggettivamente appropriabili e cose oggettivamente inappropriabili in senso assoluto. Esistono cose di cui è più facile, in linea di fatto, riservare l'uso e il godimento a un singolo soggetto, escludendone gli altri, e cose rispetto a cui tale riserva e la corrispondente esclusione sono, sempre in linea di fatto, più difficili. […] Dal punto di vista giuridico, poi, una cosa è appropriabile o non appropriabile, se esiste o non esiste un precetto, una regola, una norma […] [che, a sua volta,] dipende ovviamente da una valutazione degli organi preposti in ciascun ordinamento alla formazione del diritto.

istituzioni europee consentano di auspicare, prima ancora che immaginare, un futuro fatto di pretese di esclusivo godimento sui dati, neppure da parte del titolare del trattamento[97]. Ciò in quanto, il riconoscimento di prerogative dominicali sui dati personali (propri o altrui) avrebbe l'ineludibile effetto di erigere indesiderate barriere alla libera circolazione dei dati, fattore determinante per il rafforzamento dell'economica dei dati e, di conseguenza, del mercato unico digitale[98].

A tale considerazione, i promotori dell'approccio dominicale oppongono che, perlomeno dal punto di vista dei soggetti interessati, riconoscere la proprietà sui propri dati personali sia strumentale al coinvolgimento dei singoli nel circuito delle ricchezze generate a partire (anche) dal proprio patrimonio informativo[99]. Tuttavia, la già menzionata impossibilità dogmatica di trapiantare tale impostazione nell'ordinamento eurounitario ha indotto parte della dottrina a promuovere il raggiungimento di un analogo (e indubbiamente auspicabile) livello di coinvolgimento degli interessati rafforzandone la consapevolezza del valore monetario dei propri dati attraverso una proposta di integrazione dei doveri informativi del titolare con l'obbligo di comunicare agli

---

Questi terranno conto della minore o maggiore o anche massima difficoltà di riservare l'uso o un certo uso e la disposizione o una certa disposizione della cosa a singoli soggetti, ma inoltre soprattutto delle ragioni etiche, sociali, economiche, in definitiva politiche che possono indurre a stabilire o non stabilire con gli opportuni mezzi giuridici quella riserva a favore di dati soggetti".

[97] Così, da ultimo, "l'attuazione di un quadro legislativo abilitante per la governance di spazi comuni europei di dati" prevista per il quarto trimestre del 2020 e fissata tra le priorità per la creazione di "uno spazio europeo di dati". COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia europea per i dati* (Bruxelles, 19 febbraio 2020) (COM(2020) 66 final).

[98] Come già osseravato in dottrina, infatti, "*the new property system would introduce significant "friction" to a market that currently operates without it. This friction may be justifiable as a way to force data compilers to internalize certain costs they currently impose on others, but it is fair to say that the costs of establishing new procedures and implementing them would be far from trivial for both companies and for individuals. Collectors of personal data would presumably have to pay individuals for rights to process the data; this cost would unquestionably have to be passed on to others in the form of higher prices for the firms' own products or services, and establishing an enforcement system would also be costly. Property rights systems are not costless*." P. SAMUELSON, Privacy as Intellectual Property, cit., 1137-1138. Cfr. C.M.V. BARRAD, Genetic Information and Property Theory, 87, *Nw. U. L. Rev*., 1993, 1037, 1062-63; M.J. RADIN, Property Evolving in Cyberspace, 15, *J.L. & Com*., 1996, 509ss.

[99]Sul fallimento di mercato creato dall'assenza di un potere di contrattazione sui propri dati da parte degli interessati, con conseguente possibilità per i titolari di internalizzare tutti i proventi ritratti dal trattamento dei dati e, allo stesso tempo, esternalizzare (almeno) parte delle perdite ascrivibili ad eventuali accessi non autorizzati o episodi di c.d. *overdisclosure* si veda P.P. SWIRE, R.E. LITAN, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998, *passim*. Sui vantaggi del riconoscimento di prerogative dominicali sui propri dati si vedano, fra gli altri, C. PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, in L. GUIBAULT, P.B. HUGENHOLTZ (a cura di), *The Future of the Public Domain. Identifying the Commons in Information Law*, The Hague, Kluwer Law International, 2006, 230ss. *Contra* L. DETERMANN, No One Owns Data, cit., 35; M.J. RADIN, A Comment on Information Propertization and Its Legal Milieu, 54, *Clev. St. L. Rev*., 2006, 23ss.

interessati il prezzo (espresso in euro-dollari/mese per persona) dei dati che gli stessi "cedono" (*rectius* reificano) prestando il loro consenso al trattamento o comunque usufruendo del servizio offerto[100].

Peraltro, pur a voler ammettere che gli interessati possano *de iure condendo* vantare un diritto a ricevere (e non solo conoscere) il prezzo effettivo dei propri dati, la perdita sostenuta dai titolari non potrebbe che essere traslata sul costo di beni e servizi, finendo sostanzialmente per neutralizzare il vantaggio economico asseritamente apportato all'interessato. Inoltre, la crescente disponibilità e capacità di raccolta a basso costo di informazioni spontaneamente create in rete dagli utenti, e la sempre più accentuata capacità di inferire molte delle informazioni necessarie da una pletora sempre più ridotta di cc.dd. *raw Big Data*, fa sì che il prezzo del singolo dato decresca esponenzialmente[101].

Infine, l'assunto per cui costruire un potere dominicale sui propri dati aumenti il controllo dei singoli sul proprio patrimonio informativo e, di conseguenza, rafforzi il regime di protezione dei propri dati, è del tutto indimostrato. Al contrario, anzi, sin dagli albori del nuovo millennio acuti interpreti dell'evoluzione giuridica innescata dall'avvento di Internet e della conseguente era digitale notavano come la concezione della privacy in termini di diritto della personalità volto a conferire controllo sull'utilizzo dei propri dati (c.d. "*privacy-control*") avrebbe finito per stimolare una logica dominicale nella circolazione dei dati personali e la loro conseguente mercificazione[102]. Peraltro, la

[100] Come osservato dalla dottrina richiamata, infatti, la variabilità dei gusti, delle preferenze e, più genericamente, della personalità degli interessati, rende il singolo dato un bene a rapida obsolescenza e, di conseguenza, dotato di un valore a rapida variabilità (c.d. prodotto dinamico). G. MALGIERI, Pricing Privacy, *Computer law & security review*, 34, 2018, 289, 295. Cfr. B. H.M. CUSTERS, H. URSIC, Big Data and data re-use: a taxonomy of data re-use for balancing Big Data benefits and personal data protection, 6, *International Data Privacy Law*, 2016, 1, 4ss.

[101] B.H.M. CUSTERS, Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self- Determination, *Privacy Observatory Magazine*, 3, 2012 e G. MALGIERI, Pricing Privacy, cit., 294.

[102] Nelle parole dell'Autore: "[*t*]*he idea that one has a right to control her data leads inexorably to the concept of a trade in personal information. Instead of protecting privacy through the privacy tort, we are to safeguard it through a property regime and recourse to a privacy market*." P.M. SCHWARTZ, Internet Privacy and the State, cit., 830. In senso analogo si è espressa anche Pamela Samuelson, osservando come "[*a*]*s difficult as it may be for the average person to judge the risks of personal data misuse as a general matter, it may be even more difficult for the average person to judge the risks of selling her property rights in personal data. Data collectors may well insist on broad transfers of all of a person's right, title and interest in her personal data. While such a broad transfer works very well in a sale of a used car or a house, it may be troublesome in the context of personal data. As a result of such a transfer, an individual could potentially be foreclosed from any control over these data in the hands of the transferee or in the hands of other firms to whom the data might have been transferred. The individual could even be precluded from engaging in further transactions to sell the same data to other firms because her rights in the data*

tendenza a promuovere un approccio soggetto-centrico nella formulazione del diritto alla protezione dei dati personali già oltre un ventennio fa suscitava le perplessità di chi nutriva forti dubbi circa la capacità dei singoli di esercitare in modo pieno ed effettivo quella "*individual stewardship of personal data*" di cui sono stati progressivamente investiti da legislatori e interpreti al fine di favorirne un attivismo consapevole (*rectius* informato), poi tradottosi nel notorio strumento del consenso, funzionale all'implementazione di un regime di protezione dei dati personali declinato in termini di autodeterminazione informativa[103].

Proprio da quest'ultimo punto di vista, infatti, una delle principali critiche mosse alla tesi della c.d. *privacy-control* è quella della trappola dell'autonomia, riguardata come "l'insieme delle conseguenze scaturenti dall'affidamento al paradigma del controllo sui dati personali nello spazio cibernetico"[104] ed individuabili nelle tradizionali asimmetrie informative alimentate dalla vaga oscurità delle privacy *policies*[105], nella diffusa inerzia con cui gli utenti tendono ad accettare passivamente le impostazioni di privacy predefinite dal titolare del trattamento (c.d. *bounded rationality*[106]) e nella difficoltà registrata nel processo di sensibilizzazione di una massa sufficientemente critica di utenti tale da innescare prassi imprenditoriali maggiormente attente alle preferenze mostrate dai propri clienti in punto di trattamento dei propri dati personali[107].

Sebbene i fattori della trappola dell'autonomia sin qui richiamati, nel corso del ventennio appena trascorso abbiano subito un processo di forte attenuazione attraverso,

---

now belong to a personal data aggregator." P. SAMUELSON, Privacy as Intellectual Property, cit., 1145. Al contrario, per voci di supporto a siffatta accezione di protezione dei dati personali, si vedano, senza pretesa di esaustività, le autorevoli posizioni assunte da A. WESTIN, *Privacy and Freedom*, cit. nella parte in cui definisce il diritto alla protezione dei dati come l'aspirazione ad autodeterminare tempi, modi e misura della circolazione del proprio patrimonio informative. Pongono l'accento sulla dimensione del controllo sui propri dati, piuttosto che sull'assenza degli stessi anche C. FRIED, Privacy, 77, *Yale L.J.*, 1968, 475, 482; K. GOIMLEY, One Hundred Years of Privacy, *Wisc. L. Rev*., 5, 1992, 1335, 1356; F. SCHAUESR, Internet Privacy and the Public-Private Distinction, 38, Jurimetrics, 4, 1998, 555, 556. In senso analogo, assimila il diritto di accesso ad uno strumento legislativo di estrinsecazione del "permanente controllo del sé elettronico" S. RODOTÀ, *Il diritto di avere diritti*, Roma, Laterza Editori, 2015, 170.

[103] P.M. SCHWARTZ, Internet Privacy and the State, cit., 820. Cfr. W.W. FISHER III, Property and Contract on the Internet, 73, *Chi.-Kent L. Rev*., 1998, 1203ss.

[104] Così P.M. SCHWARTZ, Internet Privacy and the State, cit., 821.

[105] Cfr. J.R. REIDENBERG, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80, *Iowa L.Rev*., 1995, 497ss; N. WEINSTOCK NETANEL, Cyberspace Self-Governance: 4 Skeptical View from Liberal Democratic Theory, 88 *Cal. L. Rev*., 2000, 395ss.

[106] D.M. KREPS, Bounded Rationality, 3, *The New Palgrave Dictionary of Economics and the Law*,168ss.

[107] P.M. SCHWARTZ, Internet Privacy and the State, cit., 822-824. Cfr. C.R. SUNSTEIN, *Free Markets and Social Justice*, Oxford, Oxford University Press, 1997, 59ss; N. WEINSTOCK NETANEL, Cyberspace Self-Governance: 4 Skeptical View from Liberal Democratic Theory, cit., *passim*.

rispettivamente: (i) l'introduzione di più dettagliati obblighi informativi vincolati a specifici standard di trasparenza e intellegibilità; (ii) la normativizzazione di quel connubio tra tecnica e diritto sfociato nella disciplina della *privacy by design* e *by default*; nonché (iii) il rafforzamento del ruolo di supporto dell'interessato assegnato ad associazioni di categoria, autorità di vigilanza e organismi di certificazione; non lo stesso può invece dirsi per un'altra importante concausa storicamente ricondotta al fenomeno della trappola dell'autonomia: la c.d. "*data seclusion deception*".

Quest'ultima, intesa come la fallacia del paradigma della privacy come autodeterminazione informativa imputabile alla prevalenza di contrapposte esigenze collettive legate al corretto funzionamento del processo democratico (c.d. "*public accountability*") e allo svolgimento di funzioni amministrative (c.d. "*bureaucratic rationality*")[108], sembrerebbe aver subito un processo evolutivo opposto e ben rappresentato dall'ampliamento delle basi giuridiche per il trattamento lecito dei dati personali e dal conseguente ridimensionamento del ruolo di un consenso, peraltro, mai uscito dalla spirale discendente della sua inefficacia nonostante gli innegabili sforzi compiuti dal legislatore euronitario[109].

Ciò posto, non si vede come riconoscere un diritto di proprietà sui propri dati personali sia economicamente desiderabile, prima ancora che giuridicamente sostenibile, essendo al contrario storicamente dimostrata l'incapacità degli interessati di sfruttare i dispositivi di responsabilizzazione nel tempo introdotti dal legislatore eurounitario (primo fra tutti quello del consenso) in ottica di rafforzamento del proprio controllo sui dati immessi nel circuito dell'economia digitale.

Escluso così che il titolare possa *de iure condito*, né tantomeno *de iure condendo*, acquistare un diritto di proprietà sui dati altrui a titolo derivativo, e dimostrata la

[108] P.M. SCHWARTZ, Internet Privacy and the State, cit., 828ss. Interessante, in quest'ottica, la posizione assunta A. ETZIONI, *The Limits of Privacy*, New York, Basic Books, 1999, 108ss nel sostenere come un'eccessiva deferenza alle esigenze di riservatezza e protezione dei dati personali finirebbe per tradursi in un irragionevole sacrificio delle altre contrapposte esigenze della collettività, generalmente ascrivibili al "bene comune" e perciò riconducibili ad una "nuova concezione comunitaria della privacy" recentemente riacutizzatasi per effetto dell'emergenza sanitaria e ampiamente derogatorio del tracciamento e trattamento dei dati sanitari emerso nel contesto pandemico e ben enucleato nel concetto di "privacy cooperativa" recentemente coniato da CARMELITA CAMARDI in ID., C. TABARRINI, *Contact tracing* ed emergenza sanitaria. ''Ordinario'' e ''straordinario'' nella disciplina del diritto al controllo dei dati personali, 3, *La Nuova Giurisprudenza Civile Commentata*, 2020, 32, 37ss.

[109] Sull'evoluzione dei requisiti del consenso e dei tentativi di rafforzamento del suo carattere libero e specifico si vedano le più ampie riflessioni compiute *infra sub* Cap. II §2.3.

propensione del legislatore a contrastare forme di godimento esclusivo sui dati personali (specialmente altrui) ben rappresentata dal nuovo istituto della portabilità dei dati e dalla sua strumentalità a smantellare pericolosi monopoli informativi da parte dei *BigTechs*[110], risulta altrettanto insostenibile la configurabilità di forme di acquisto a titolo originario di diritti di proprietà sui dati personali altrui. Come già rilevato da risalente e autorevole dottrina, infatti, trasfigurare le caratteristiche proprie di un istituto nato per tutelare il rapporto diretto ed immediato instaurato dal proprietario con la cosa materiale, adattandone le tecniche di protezione dell'uso esclusivo a beni aventi caratteristiche del tutto diverse da quello per cui il diritto reale è stato concepito, significa chiamare proprietà un rapporto giuridico totalmente diverso[111].

È pur vero, però, che la proprietà è soltanto uno degli strumenti legislativi a tutela di forme di godimento esclusivo. Un'altra importante corrente dottrinale, infatti, sostiene la configurabilità di forme di proprietà intellettuale sui propri dati personali[112]. È a tali riflessioni che verrà quindi dedicato il prossimo paragrafo, al fine di saggiarne la sostenibilità anche e soprattutto nella prospettiva del titolare del trattamento.

[110] Cfr. COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI, *Una strategia europea per i dati* (Bruxelles, 19 febbraio 2020) (COM(2020) 66 final); M. GIORGIANNI, Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato, *Contratto e impresa*, 4, 2019, 1387ss; G.M. RICCIO, F. PEZZA, *Portabilità dei dati e interoperabilità*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 406-409; L. BIANCHI, Il diritto alla portabilità, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 228ss; E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 212ss; P. DE HERT, V. PAPAKONSTANTINOU, G. MALGIERI, L. BESLAY, I. SANCHEZ, The right to data portability in the GDPR: Towards user-centric interoperability of digital services, 34, *Computer Law & Security Review*, 2, 2018, 193ss.

[111] Cfr. V. SCIALOJA, *Teoria della proprietà nel diritto romano*, 29; S. PUGLIATTI, *La proprietà nel nuovo diritto*, 250; O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, *cit.*, 181.

[112] Cfr. O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, *cit.*, 193 ove sottolinea come l'ostinazione ermeneutica verso il riconoscimento di diritti di proprietà su beni immateriali spesso si traduca in una petizione di principio e finisca trascurare altri strumenti normativi più adatti a salvaguardare forme di godimento più o meno esclusivo sugli stessi.

1.5. Una prospettiva industrialista: dal diritto morale d'autore alla "quasi proprietà" (intellettuale) sul dato personale

La rilevata impossibilità dogmatica di svincolare l'istituto della proprietà da quella materialità del suo oggetto che ne ha storicamente plasmato il contenuto, associata all'inopportunità economica di legare i dati personali a regimi di circolazione suscettibili, da un lato, di mercificare tratti della personalità degli interessati e, dall'altro, di erigere indesiderate barriere alla libera circolazione dei dati personali, nel mettere in luce l'inadeguatezza di approcci dottrinali di stampo dominicale non ha eliminato l'esigenza di conferire una razionalità giuridica al mercato dei dati[113].

A tal riguardo, parte della dottrina, rilevando come la fisiologica non rivalità dei dati sia stata in parte soppiantata da una loro artificiosa "scarsità" per effetto della formazione di monopoli informativi da parte dei *BigTechs*[114], ha proposto di contrastare tale fenomeno di appropriazione *de facto* dei patrimoni informativi individuali reinterpretando la posizione degli interessati secondo una logica propria del modello della proprietà intellettuale o, in alternativa, della quasi proprietà (intellettuale)[115].

La scelta legislativa di tipizzare un *numerus clausus* di diritti di proprietà intellettuale rende tale operazione ermeneutica già in premessa particolarmente

[113] In senso analogo si è espresso J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, *Diritto del Commercio Internazionale*, 4, 2017, 831, 840 che, dopo aver riepilogato in prospettiva comparativa i vari approdi dottrinali in punto di "proprietà" sui dati personali, nota come "[*t*]*hese positions reflect that the current debates still are permeated by a material/immaterial goods distinction hardly fitting to the new types of digital objects of private law relations (information, personal data, virtual items, in-app purchases, crypto currencies etc.), which have emerged and escape the above-mentioned dichotomy*." Cfr. P. PALKA, Redefining «property» in the Digital Era. When online, do as the Romans did, 8, *EUI Working Paper Law*, 2016, 7 ss.

[114] Come già rilevato, infatti, "*excludability is a reality, even considering all technological infrastructures and encryption techniques capable to restrict access to personal data. However, studies in law and economics confirm that if de facto property rights are not assigned by a legislative recognition, they will be allocated in a way that is proportionate to the ability to exclude others from that resource*." G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, 20, *Journal of Internet Law*, 5, 2016, disponibile su *https://papers.ssrn.com/abstract_id=2916079*, 7 . Cfr. O. Tene, J. Polonetsky, *Big Data* for All: Privacy and User Control in the Age of Analytics, 11, *Nw.K. Tech. & Intell. Prop*., 2013, 239, 255ss; C. PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, cit., 229ss.

[115] Analogamente si è espresso CIANI, sottolineando come "*if property rights on data are not assigned by a legislative action, data will probably be de facto appropriated by more powerful actors. Therefore, maintaining that personal data is res nullius (or nobody's property) would be an illusion and would be equivalent to assign ownership to the information industry*." ID., Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 841. Cfr. G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, cit., *passim*; N. PURTOVA, The Illusion of Personal Data as No One's Property, cit., *passim*; D.L. ZIMMERMAN, Livinig Without Copyright in a Digital World, 70, *Albany Law Review*, 2007, 1375ss.

complessa ma, cionondimeno, meritevole di approfondimento in ragione della sua potenziale attitudine a realizzare un efficace connubio tra i connotati personalistici e reali caratterizzanti il fenomeno della circolazione dei dati personali[116].

In particolare, ci si è in primo luogo interrogati circa la configurabilità, in capo al soggetto interessato, di un diritto morale d'autore sui propri dati personali[117]. Tale soluzione, infatti, consentirebbe di valorizzare il perpetuo vincolo personalistico che lega l'informazione contenuta nel dato personale al soggetto interessato a cui si riferisce senza, allo stesso tempo, sacrificare le esigenze di alienabilità (*rectius* circolazione) dello stesso. In quest'ottica, guardare al dato personale come oggetto di licenze d'uso (peraltro non necessariamente esclusive[118]) realizzerebbe una soltanto parziale mercificazione del dato[119].

Tale soluzione, per quanto astrattamente più coerente alla natura immateriale del dato e alla dicotomia persona-merce connaturata allo stesso[120], mal si concilia con la *ratio* utilitarista che muove l'istituto del diritto d'autore: incentivare investimenti personali e

---

[116] Sulla natura *sui generis* del diritto d'autore si vedano, fra gli altri, le riflessioni di N. STOLFI, *Il diritto di autore*, Milano, Società Editrice Libraria, 1932, 1ss. Cfr. U. NATOLI, *La proprietà*, Milano, Giuffré, II ed., 1976, 84ss; O.T. SCOZZAFAVA, *I beni e le forme giuridiche di appartenenza*, *cit*., 460; G. FINOCCHIARO, *Sistema di diritto industriale*, Vol. I, Padova, Cedam, 1932, 183 ss.; F. CARNELUTTI, *Usucapione della proprietà industriale*, cit., 26ss; L. FERRARA, *Il diritto reale di autore in rapporto alla nuova legge italiana*, Napoli, Jovene, 1940, *passim*; M. ARE, L'oggetto del diritto di autore, Milano, Giuffré, 1963, 290ss; G. COTTINO, *Diritto commerciale*, I, Padova, Cedam, 1976, 210 ss; J. RITTER, A. MAYER, Regulating Data as Property. A New Construct for Moving Forward, 16, *Duke L & tech Rev*, 2018, 220ss.

[117] Cfr. J.M. VICTOR, The Eu General Data Protection regulation: Toward a Property Regime for Protecting Data Privacy, cit., 524.

[118] Così si esprime, ad esempio, Instagram nelle sue condizioni d'uso ove chiarisce come la piattaforma "[n]on rivendi[chi] la proprietà di eventuali contenuti pubblicati dall'utente sul Servizio o tramite lo stesso. Al contrario, quando l'utente condivide, pubblica o carica un contenuto coperto da diritti di proprietà intellettuale (ad es. foto o video) in relazione o in connessione con il nostro Servizio, ci concede una *licenza non esclusiva, non soggetta a royalty, trasferibile, conferibile in sottolicenza e globale per la trasmissione, l'uso, la distribuzione, la modifica, l'esecuzione, la copia, la pubblica esecuzione o la visualizzazione, la traduzione e la creazione di opere derivate dei propri contenuti* (nel rispetto delle impostazioni di app e privacy). L'utente può revocare questa licenza in qualsiasi momento eliminando i propri contenuti o il proprio account. Tuttavia, i contenuti potrebbero continuare a essere visibili in caso di condivisione e mancata eliminazione da parte di altri." (corsivo aggiunto) Condizioni d'uso della piattaforma Instagram disponibili all'indirizzo *it.facebook.com/help/instagram*. Sul punto già G. MALGIERI, Pricing Privacy, cit., 294.

[119] Parla, in questo senso, di beni "*incompletely commodified*" nel senso di "*neither fully commodified nor fully removed from the market*" M.J. RADIN, *Contested Commodities. The Trouble with Trade in Sex, Children, Body Parts and Other Things*, Cambridge (MA), Harvard University Press, 1996, 20.

[120] Sull'attitudine della proprietà intellettuale a dare maggior risalto alla dimensione personalistica della dignità dell'individuo v. anche J. ROTHMAN, The Inalienable Right of Publicity, 101, *Georgetown Law Journal*, 2012, 185ss. *Contra* H. BEWERLY-SMITH, A. Ohly, A. Lucas-Schloetter, *Privacy, Property and Personality. Civil Law Perspective on Commercial Appropriation*, Cambridge Studies in Intellectual Property Rights, Cambridge, Cambridge University Press, 2005, 48ss.

patrimoniali nella produzione di opere d'ingegno che, in ragione della loro originalità, possono contribuire al migliore sviluppo tecnologico e culturale della società[121]. Logica, questa, evidentemente estranea alle dinamiche che muovono il mercato dei dati. Per quanto espressione della personalità della persona fisica da cui promanano, infatti, è difficile individuare nel processo di creazione (*rectius* raccolta) dei dati un'attività creativa degli interessati meritevole di tutela ai sensi della normativa sul diritto d'autore[122]. Peraltro, pur volendo ascrivere alla disciplina in questione una inesistente funzione di tutela della personalità dell'autore, il riconoscimento di un siffatto diritto in capo al soggetto interessato avrebbe poco senso in ottica di protezione dei suoi dati personali, in quanto funzionale alla realizzazione di interessi di circolazione e remunerativà più coerenti al contenuto di quel diritto al trattamento dei dati altrui sin qui ricostruito in capo al titolare[123].

Ciononostante, a dispetto dell'affinità teleologica che lega il diritto d'autore alla logica propria del versante industriale del mercato dei dati, neppure l'attività di predisposizione dei mezzi e delle finalità del trattamento, così come quella di raccolta e

[121] Chiare, in questo senso, le parole di DETERMANN per cui "[*a*]*lthough there are different philosophical foundations of copyright law, the predominant philosophical framework undergirding American copyright law is utilitarian: "The immediate effect of our copyright law is to secure a fair return for an 'author's' creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good."* […] *Yet, except for exclusion rights, data protection and privacy laws diverge from property laws. Privacy laws do not incentivize or reward creation or investment, do not regulate the acquisition or transfer of ownership rights to others, and do not apply against everyone. Instead, EU data protection laws confer exclusion rights against governments and businesses, but not against individuals acting for personal or household purposes*." L. DETERMANN, No One Owns Data, cit., 18 e 25. Per una concezione del diritto morale d'autore sul dato personale come un modello proprietario alternativo legato al presupposto giuridico-ideologico per cui le creazioni d'ingegno sono espressione della personalità dell'autore, ma volto ad incentivare investimenti e non a proteggere diritti della personalità dei titolari v. P. SAMUELSON, Privacy as Intellectual Property, cit., 1147.

[122] Come già osservato in dottrina "*[t]he creation and dissemination of personal data does not generally promote "science" in the constitutional sense (i.e., knowledge), nor does it promote technological innovation. Indeed, the purpose of the proposed new personal data property right is almost the inverse of traditional intellectual property law, for it would grant a property right in order to restrict the flow of personal data to achieve privacy goals*." L. DETERMANN, No One Owns Data, cit., 1141-1143. Cfr. S.G. DAVIES, Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology & Privacy*, Cambridge (MA), MIT Press, III ed., 2001, 161 ove si definisce espressamente il processo di mercificazione dei dati personali come "*inimical to privacy*".

[123] In senso analogo si è espresso Zeno Zencovich, notando come "la principale esigenza di protezione dei dati personali è quella di mantenerne la riservatezza impedendone la circolazione; mentre — come è noto — nel sistema delle privative industriali la contropartita della protezione accordata dall'ordinamento è la pubblicità dell'invenzione o dell'opera attraverso la procedura, essenziale, del deposito o della pubblicazione. Assai più convincente — e generalmente già recepita — è la qualificazione del diritto di esclusiva sui propri dati personali come diritto della personalità e più precisamente come espressione della riservatezza." V. ZENO-ZENCOVICH, Informazione (profili civilistici) (voce), cit., § 5.

analisi dei dati, presenta quei tratti di originalità e creatività propri delle opere d'ingegno, in quanto prevalentemente meccanica e automatizzata. Ne consegue che, come già da tempo rilevato da autorevole dottrina, "[l]a singola informazione non è suscettibile di essere qualificata come opera dell'ingegno. Sarà semmai un insieme di informazioni, purché il modo di raccolta, classificazione e presentazione risponda ai requisiti di creatività imposti in genere dalle leggi e dalle convenzioni sul diritto d'autore[124]."

È così, quindi, che l'attenzione della dottrina si è spostata sulla tutela potenzialmente apprestata al complessivo patrimonio informativo individuale, e collettivo, dalla disciplina dettata dalla Direttiva 96/9/CE del Parlamento Europeo e del Consiglio dell'11 marzo 1996 relativamente alla tutela giuridica delle banche di dati. Più specificatamente, escluso, per le medesime ragioni sin qui richiamate, che l'insieme dei dati personali di un soggetto interessato, così come dei dati personali di più interessati raccolti dal titolare, possano costituire un'opera d'ingegno tutelata ai sensi del diritto d'autore in ragione della (non) creatività della scelta o disposizione del materiale informativo ivi contenuto *ex* art. 3 par.1 Dir. 96/9/CE, la dottrina si è interrogata sulla configurabilità di un diritto "*sui generis*" su quest'ultimo ai sensi dell'art. 7 Dir. 96/9/CE.

Ciò in quanto, sebbene le tecniche automatizzate di *data analytics* rendano quantomeno trascurabile (se non del tutto assente) il contributo "creativo" degli operatori umani nella selezione e organizzazione dei dati personali raccolti, gli investimenti compiuti dal titolare per dotarsi di un siffatto apparato di c.d. *data-driven innovation*, ove rispettosi di quello standard di rilevanza "sotto il profilo qualitativo o quantitativo" prescritto dalla Dir. 96/9/CE, potrebbero giustificare il riconoscimento del diritto del titolare, in qualità di costitutore di una siffatta banca dati, di vietare operazioni di estrazione e/o reimpiego della totalità o di una parte qualitativamente o quantitativamente sostanziale della stessa[125].

[124] Ancora, puntualizzava l'Autore, *Ibid*. In senso analogo si è espressa la giurisprudenza statunitense nel caso *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975) richiamata anche da DETERMANN nell'osservare come "[*c*]*opyright law can provide property rights to original works of authorship that contain information, including creative compilations of data, but not to the underlying data itself*.". L. DETERMANN, No One Owns Data, cit., 18. Cfr. P.S. MENELL, M.A. LEMLEY, R.P. MERGES, *Intellectual Property in the New Technological Age*, Vol. I, Clause 8 Publishing, 2019, 541ss.

[125] Cfr. J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 833. Sull'esigenza di remunerare l'attività di raccolta e organizzazione del contenuto di banche dati G. PALAZZOLO, La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (UE) n. 2016/679, *Contratto e impresa*, 2017, 613ss.

Tale impostazione ermeneutica avrebbe il vantaggio di salvaguardare un grado di godimento esclusivo sui dati raccolti in capo al titolare compatibile con i diritti di accesso degli interessati ai singoli frammenti della banca dati ad essi riferibili. Tuttavia, come osservato da costante giurisprudenza della Corte di Giustizia dell'Unione europea[126], e come ribadito da recente dottrina[127], la tutela *sui generis* opera soltanto nel caso in cui la creazione della banca dati rappresenti la principale componente dell'attività imprenditoriale del suo costitutore (restando quindi esclusi i cc.dd. *spin-off databases*) e gli investimenti allo scopo sostenuti abbiano riguardato esclusivamente l'attività di selezione/organizzazione e non anche generazione del contenuto della banca dati.

Anche tale disciplina risulta sostanzialmente inadeguata al contesto *Big Data* nella misura in cui, anche a voler assumere che gran parte dei dati raccolti dai titolari siano generati direttamente dagli interessati (ad esempio con i loro comportamenti in rete, come nel caso degli *user-generated contents*) e quindi soltanto selezionati dai primi, la maggior parte degli operatori coinvolti nel mercato dei dati sfruttano il vantaggio competitivo offerto dalle più avanzate tecniche *di Big Data Analytics* soltanto in via strumentale al perfezionamento delle strategie di *marketing, customer experience* e *product development* della diversa e principale attività commerciale svolta. È questo, tra l'altro, il caso di tutti i *BigTechs* che, a partire da Amazon e Facebook, hanno rafforzato la propria posizione di mercato proprio grazie agli imponenti monopoli informativi acquisiti attraverso la raccolta e l'analisi dei dati dei propri utenti nel contesto e in via strumentale alla redditività della diversa attività svolta in via principale[128].

[126] Cfr. Sentenza della Corte di giustizia dell'Unione europea (Terza Sezione) del 1 marzo 2012, *Football Dataco Ltd e altri contro Yahoo! UK Ltd e altri*, ECLI:EU:C:2012:115; Sentenza della Corte di giustizia dell'Unione europea (grande sezione) del 9 novembre 2004, *The British Horseracing Board Ltd e altri contro William Hill Organization Ltd*., ECLI:EU:C:2004:695; *Final Commission Working Staff Document on the Free Flow of Data and Emerging Issues of the European Data Economy* (COMMISSIONE EUROPEA, 10 gennaio 2017) (COM(2017) 9 final), 20ss.

[127] J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 837.

[128] Cfr. V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, Giuffré, 2017, *passim*; D.C. Nunziato, With Great Power Comes Great Responsibility: Proposed Principles of Digital Due Process for ICT Companies, in in L. FLORIDI (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, Vol. 17, Law, Governance and Technology Series, Springer, Cham, 2014, 68ss; F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015, 141ss; B. PRAINSACK, *Data Donation: How to Resist the iLeviathan*, in J. KRUTZINNA, L. FLORIDI (a cura di), *The Ethics of Medical Data Donation*, Philosophical Studies Series, Vol. 137, Cham, Springer Open, 2019, 11ss.

La rilevata inadeguatezza, peraltro, risulta ulteriormente aggravata ove si prenda atto del vuoto di tutela che tale interpretazione della Dir. 96/6/CE lascerebbe attorno al regime di circolazione dei cc.dd. metadati creati dal titolare del trattamento attraverso le inferenze rilevate nel corso del processo di analisi dei dati personali raccolti. Tali "*intellectually integrated data*"[129], sui quali si ritornerà meglio a breve, non soltanto rappresentano il principale fattore di redditività del mercato dei dati, ma sono anche uno dei principali elementi informativi coinvolti nei processi decisionali automatizzati. Per questo motivo, ai fini di una corretta impostazione dell'analisi che verrà svolta nei prossimi capitoli, particolare importanza riveste la terza (e ultima) corrente dottrinale "industrialista" che ha teorizzato la possibilità di proteggere il dato personale alla stregua di un segreto commerciale.

A tal riguardo, recente dottrina ha ravvisato nella disciplina sui segreti commerciali lo strumento legislativo più adeguato a realizzare una c.d. *sensitive commodification*[130] del dato personale attraverso la creazione di un regime di "quasi proprietà" definito come un "*relational entitlement to exclude—the right to exclude specific actors from a resource given a specific event, a given type of behavior, and/or a given relationship between the actors*. [131]"

In quest'ottica, il segreto commerciale rappresenterebbe una declinazione della macrocategoria della quasi proprietà[132] che, collocandosi al confine tra la logica normativa della proprietà intellettuale e del diritto della concorrenza[133], si

[129] G. MALGIERI, Trade Secrets v Personal Data: a possible solution for balancing rights, *International Data Privacy Law*, 6, 2016, 102, 115; B. REDDIX-SMALLS, Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market, 12, U.C. Davis Bus. L.J., 2011, 87ss.

[130] G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, cit., 15ss; S. BALGANESH, Quasi-Property: Like, but not Quite Property, 160, *U. Penn. Law Rev*., 2012, 1891ss, *passim*; L.H. SCHOLZ, Privacy as Quasi-Property, 101, *Iowa Law Review*, 2016, 1113ss, *passim*, 12; P. SCHWARTZ, Property, Privacy and Personal Data, 117, *Harv. L. Rev*., 2004, 2055, 2060ss.

[131] G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, cit., 19 citando L.H. SCHOLZ, Privacy as Quasi-Property, cit., 1115. In senso analogo, parla di "*relational entitlement*" N. PURTOVA, The Illusion of Personal Data as No One's Property, cit., 94.

[132] G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, cit., 19 spec. nt. 116 ove richiama la qualificazione del segreto commerciale ad una quasi-proprietà operata dai giudici californiani in O'Grady v Superior Court, 44 Cal. Rptr. 3d 72, 112 (Ct. App. 2006). Cfr. R.G. BONE, A New Look at Trade Secret Law: Doctrine in Search of Justification, 86, *Calif. L. Rev*., 1998, 241ss.

[133] Più specificatamente è stato osservato come "[*a*]*lthough courts have sometimes loosely referred to trade secrets as the "property" of the firm that licensed them and have on occasion held trade secrets to be property for certain purposes, the more appropriate way to characterize the firm's interest in a trade*

caratterizzerebbe per una flessibilità tale da renderlo, da un lato, suscettibile di avere ad oggetto beni immateriali di natura informativa e, dall'altro, più conforme alle esigenze di controllo sulla limitazione della circolazione dei propri dati personali di cui dall'articolo 8 della Carta di Nizza. Ciò in quanto il carattere c.d. "statico" dell'interesse tutelato con la Dir. 2016/943/UE, a differenza del diritto d'autore, mira a salvaguardare la segretezza del patrimonio informativo oggetto di tutela e non a favorirne la circolazione in nome del progresso sociale[134].

Un altro vantaggio da alcuni associato all'opzione ermeneutica della quasi proprietà sui dati personali è la sua capacità di preservare un certo grado di "fluidità della *res*" che ne forma oggetto, offrendone un criterio di individuazione che, muovendosi per classi e caratteristiche generali, lascia aperta la pletora di risorse immateriali potenzialmente idonei ad ottenerne tutela[135].

In questo modo, da un lato, vengono potenzialmente attratti nella sfera di esclusività tutelata dalla disciplina sui segreti commerciali anche i dati creati dai titolari e, dall'altro, si crea un sistema di licenze con cui gli interessati potrebbero gestire il regime di accesso ai dati personali in loro controllo[136].

Tale impostazione, tuttavia, è stata criticata con particolare riguardo alla difficoltà di assimilare la nozione di segretezza, propria della disciplina sulle informazioni commerciali, a quella di riservatezza, alla base dell'intero impianto normativo sulla protezione dei dati personali. In particolare, ai sensi dell'articolo 2 par.1 Dir. 2016/943/UE rientrano nella nozione di segreto commerciale soltanto quelle informazioni

secret is to say that the law protects the firm against breaches of contracts and confidential understandings, as well as against the use of improper means to obtain the secret. Despite its frequent presence in texts of intellectual property law, trade secrecy law remains firmly rooted in unfair competition law." Così L. DETERMANN, No One Owns Data, cit., 16.

[134] Cfr. G. MALGIERI, Trade Secrets v Personal Data: a possible solution for balancing rights, cit., 113; G RESTA, *Nuovi beni immateriali e* numerus clausus *dei diritti esclusivi*, in ID. (a cura di), *Diritti esclusivi e nuovi beni immateriali*, Torino, Utet, 2011, 48ss. In senso analogo, è stato sottolineato come "[*a*]*lthough trade secrecy and information privacy laws obviously differ in many significant respects, these laws nonetheless have at least three important interests in common: first, an interest in protecting the interest of the claimant to restrict access to and unauthorized uses of secret/private information; second, an interest in giving firms/individuals control over commercial exploitations of secret/private information; and third, an interest in setting and enforcing minimum standards of commercial morality*." P. SAMUELSON, Privacy as Intellectual Property, cit., 1151-1152.

[135] G. MALGIERI, "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, cit., 20.

[136] Parla di un "*system of trade secret licenses in their personal data*" P. SAMUELSON, Privacy as Intellectual Property, cit., 1151.

che: (i) non sono, nel loro insieme, generalmente note o facilmente accessibili agli altri operatori del settore; (ii) traggono il loro valore commerciale dall'essere segrete; e (iii) sono sottoposte ad adeguate misure di salvaguardia della loro segretezza da parte del soggetto che su di esse esercita legittimo controllo[137].

La dottrina si è quindi chiesta se fosse possibile ricondurre entro tali confini definitori dati personali resi spontaneamente pubblici dagli interessati e perciò liberamente accessibili da qualsiasi titolare abbia interesse al loro trattamento. Perlomeno dalla prospettiva dell'interessato, infatti, è difficile ravvisare in queste ipotesi quegli effettivi sforzi compiuti per mantenere la segretezza dei propri dati personali a cui la Dir. 2016/943/UE condiziona l'esercizio dello *ius excludendi* sui segreti commerciali[138].

La circostanza per cui il dato sia "generalmente not[o] o facilmente accessibil[e][139]" dai titolari, infatti, sebbene non faccia venir meno la protezione allo stesso apprestata dal GDPR equindi-l'illiceità di qualsivoglia trattamento non fondato su una delle basi giuridiche ivi disciplinate, fa cionondimeno dubitare della capacità della disciplina sui segreti commerciali di assurgere ad efficace modello di circolazione del dato personale nel contesto *Big Data*[140].

Tale obiezione acquista particolare pregio con riferimento a quei fenomeni di *free-riding* sussistenti ogniqualvolta la libera accessibilità di dati resi spontaneamente pubblici dagli interessati (ad esempio in contesti di *social networking*) renda concretamente inverosimile l'instaurarsi di dinamiche di mercato in cui il titolare sia disposto a pagare

[137] J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 839. Cfr. L. DETERMANN, No One Owns Data, cit., 15. Cfr. M. RISCH, Why Do We Have Trade Secrets?, 11, *Marq. Intell. Prop. L. Rev*. 1, 2007, 16-18; P.S. MENELL, M.A. LEMLEY, R.P. MERGES, *Intellectual Property in the New Technological Age*, 545 .

[138] P. SAMUELSON, Privacy as Intellectual Property, cit., 144, spec. nt 148.

[139] Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti [d'ora in avanti Direttiva 2016/943/UE], GUUE L. 157/1, Articolo 2 par. 1.

[140] In senso parzialmente contrario si è espressa Pamela Samuelson, puntualizzando come "[*t*]*he information* […] *does not become "public" simply because a number of firms possess it--as long as each is under an implicit or explicit pledge to maintain the nonpublic status of the information*." ID., Privacy as Intellectual Property, cit., 1152. Cfr. R.T. NIMMER, Breaking Barriers. The Relation Between Contract and Intellectual Property Law, 13, *Berkeley Tech. L.J.*, 1998, 827ss; L. BRENNAN, The Public Policy of Information Licensing, 36, *Hous. L. Rev*., 1999, 61ss; J.H. REICHMAN, J.A. FRANKLIN, Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information, 147, *U. Pa. L. Rev*., 1999, 875ss.

per l'accesso all'informazione (fenomeno, questo, anche noto come "*privacy externalities*")[141].

Anche guardando a tale impostazione ermeneutica dalla prospettiva che qui più interessa, ovvero quella del titolare del trattamento, risulta altrettanto complesso riconoscergli una privativa di matrice commerciale sui dati personali raccolti. Ciò non soltanto per la difficile sostenibilità giuridica del diritto a mantenere la segretezza di dati personali altrui, fortemente compromessa dai poteri di accesso e disposizione (*rectius* portabilità) che gli interessati mantengono sugli stessi[142], ma anche e soprattutto in ragione dell'indimostrato assunto per cui i dati, in quanto potenziali segreti commerciali, trarrebbero il loro valore economico dall'essere segreti[143].

Al contrario, anzi, è sempre più coralmente sostenuta l'idea che il rafforzamento del mercato unico digitale passi per la promozione della più ampia liberalizzazione della circolazione dei dati (personali e non), da alcuni allo scopo assimilati a veri e propri *commons* [144]. Peraltro, lo stesso valore monetario del dato singolarmente considerato è in

[141] G. MALGIERI, Pricing Privacy, cit., 299. Cfr. S. GNESI, I. MATTEUCCI, C. MOISO, P. MORI, M. PETROCCHI, M. VESCOVI, *My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data*, in B. PRENEEL, D. IKONOMOU (a cura di), *Privacy Technologies and Policy, Lecture Notes in Computer Science*, Berlino, Springer, 2014, 154ss.

[142] In senso contrario si è espresso MALGIERI, il quale, sostenendo la configurabilità di un segreto commerciale del titolare sul complesso dei dati personali altrui raccolti, ha individuato nella tecnica della c.d. decontestualizzazione il metodo più idoneo a bilanciare siffatta privativa con il diritto di accesso degli interessati. Nelle sue parole "*right to access and right to portability may be limited, providing only data that are necessary for the 'context' of data subjects (quality and quantity of information related to them in possession of the businesses, without all economic outputs of those data).* […] *On the other hand, customer data can be 'trade secrets' only if they are considered in their totality and in their complexity: it is obvious that single customer data (eg biographical information of one single client) are not valuable as trade secrets, and their disclosure does not adversely affect the intellectual work of the businesses*." G. MALGIERI, Trade Secrets v Personal Data: a possible solution for balancing rights, cit., 114-115.

[143] In senso critico si è espresso anche DETERMANN notando come "[*d*]*evice manufacturers typically cannot access information from devices without the device owners' consent, much less keep the information secret from the device owners. Device manufacturers thus generally cannot claim trade secret ownership rights in the data and information generated by the devices they sell to customers. Consumers also typically cannot claim trade secret rights in the data produced by the devices they own because they cannot substantiate a competitive advantage from keeping the data secret. Moreover, much of the data and information generated by cars and other connected devices, such as its location and environment, is generated and displayed in plain sight, depriving that information of secrecy. Thus, trade secret laws do not convey meaningful ownership in data, and instead, merely offer some level of protection against unfair misappropriation of information*." L. DETERMANN, No One Owns Data, cit., 16. Cfr. P. SAMUELSON, Privacy as Intellectual Property, cit., 1153-1155.

[144] In questo senso è stato sostenuto che "[*s*]*ince the marginal costs of using data by an additional user are zero, the welfare-optimal solution would be to grant general access to these data free of charge, without introducing property rights in order to protect it. This suggests that institutions others than property, such as «commons» may be more effective and the general principle of a public domain of free information should prevail over the creation of information monopolies. When there is no need to preserve a non-scarce resource, property rights might be still introduced to ensure that this resource is actually produced (as it is the case for information protected by intellectual property rights). However, this does*

costante decrescita proprio in ragione della dimensione squisitamente aggregata assunta dai patrimoni informativi utilizzati nei processi di alimentazione e "addestramento" dei sistemi automatizzati di *data analytics* implementati grazie alle riscoperte potenzialità dell'intelligenza artificiale[145].

Sebbene sul rapporto tra *Big Data* e Intelligenza artificiale si tornerà più profusamente nel prossimo capitolo, ove ne verranno analizzati i tratti salienti funzionali alle riflessioni sulla disciplina dei processi decisionali ivi condotte, è, tuttavia, fin d'ora opportuno mettere in evidenza come l'impiego sempre più diffuso di sistemi di *Machine Learning* nel trattamento dei dati personali altrui renda superflua la raccolta di un crescente numero di categorie di informazioni. Ciò in ragione della capacità dei titolari di inferire la maggior parte delle conoscenze più strategiche dal punto di vista imprenditoriale (e decisionale) in modo autonomo e automatizzato, e a partire da una varietà di cc.dd. *raw Big Data* relativamente ridotta[146].

1.5.1. Cenni di quasi proprietà sui metadati (rinvio)

È in questa prospettiva, quindi, che la disciplina dei segreti commerciali assume un'importanza centrale nel bilanciamento del diritto dell'interessato di conoscere le informazioni che il titolare utilizza per prendere decisioni unicamente automatizzate nei propri confronti e il diritto di quest'ultimo di mantenere segrete conoscenze

not seem to be an issue for data. Otherwise, creating an exclusive right in data might lead to an overly protective legal framework. Indeed, protection of data would at least indirectly affect the access to and use of information, in the same way, the copyright makes with respect of creative information. Moreover, the strengthening of market power derived from data, would entail the risk of impeding business operations of other market players who depend on access to data, and generate negative effects on the development of downstream data markets, ultimately fostering anti-competitive market entry barriers and interfering with the freedom to conduct a business and compete." J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 844. Sulla nozione di "*information commons*" definiti come "*an organization of the production and distribution of knowldge that ensures open access*" v. S. GHOSH, *How to Build a Commons: Is Intellectual Property Constrictive, Facilitating, or Irrelevant?*, in C. HESS, E. OSTROM (a cura di), *Understanding Knowledge as a Commons. From Theory to Practice*, Cambridge (MA), MIT Press, 2007, 210; C. ANGELINI, *Lo statuto dei dati personali*, cit., 77ss.

[145] Per una panoramica dei vari metodi teorizzati per la quantificazione del valore dei dati v. G. MALGIERI, Pricing Privacy, cit., 295ss.

[146] Ivi, 299. Cfr. R. VAN LOO, Making Innovation More Competitive: The Case of Fintech, 6, *UCLA L. Rev.*, 2018, 232, 242; GENEVA ASSOCIATION, *Big Data and Insurance: Implications for Innovation, Competition and Privacy*, Zurigo, 2018, 22ss; U. FAYYAD, G. PIATETSKY-SHAPIRO, PADHRAIC SMYTH, From Data Mining to Knowledge Discovery in Databases, 17, *AI Magazine*, 3, 1996, 37, 39ss.

autonomamente create (*rectius* inferite) e, stavolta sì, idonee a conferirgli un vantaggio competitivo soltanto nella misura in cui siano mantenute segrete.

Se, infatti, per tutti i motivi sin qui richiamati, è difficile configurare un diritto di proprietà, proprietà intellettuale, o quasi proprietà sul dato personale proprio o altrui, non lo stesso può dirsi con riferimento ai metadati[147].

Questi ultimi, anche definiti *modeled* o *derived data*, come già accennato, sono ascrivibili alla macrocategoria delle cc.dd. fonti "private" di produzione dei dati e sono intesi come dati creati (*rectius* inferiti) dai *data brokers* o comunque dal titolare del trattamento per il tramite dello svolgimento di analisi statistiche di complessità varia e massima nel caso di impiego di strumenti automatizzati di *predictive analytics*.[148]

I dati derivati si distinguono in cc.dd. *directly modeled data* e *look alike model data*. I primi sono costituiti da informazioni inferite statisticamente da una ampia pletora di dati "grezzi" al fine di compiere valutazioni predittive per specifiche finalità che generalmente sono riconducibili alla prevenzione di frodi e mitigazione del rischio dell'operazione oppure all'ottimizzazione delle strategie di *marketing*. I cc.dd. "*look alike models*", invece, sono frutto di analisi combinate di patrimoni informativi più limitati dal punto di vista quantitativo perché riferibili a gruppi più ristretti di utenti e quindi meno rappresentativi. Tale tipologia di informazioni, tuttavia, è particolarmente utile per inferire modelli di comportamento utili ad individuare potenziali membri del proprio *target audience*[149]. Tali prassi, di certo concettualmente antecedenti l'avvento

[147] Esprimono preferenza per la tesi della privativa industriale sui metadati a quella della proprietà sui dati V. ZENO-ZENCOVICH, Dati, grandi dati, dati granulari e la nuova epistemologia del giurista, *Rivista di diritto dei media*, 2, 2018, 1, 4; J. DREXL, Designing Competitive Markets for Industrial Data. Between Propertisation and Access, 8, *JIPITEC*, 2017, 22ss; H.R. VARIAN, Beyond *Big Data*, 49, *Business economics*, 1, 2014, 27ss.

[148] Il patrimonio informativo protagonista dell'economia dei dati è alimentato da una variegata serie di fonti di produzione dei dati in parte pubblicamente accessibili come nel caso di pubblici registri, informazioni pubblicate online senza restrizioni di accesso, ovvero raccolte attraverso sondaggi e somministrazione di questionari. A tali fonti "pubbliche" di produzione informativa si affiancano però anche quelle "private" dei dati raccolti dalle aziende nel corso dello svolgimento delle proprie attività, inclusi i cc.dd. *user-generated contents* originati per effetto della navigazione online degli utenti. Cfr. A. STAZI, F. CORRADO, Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica, *Diritto dell'Informazione e dell'Informatic*a, 2, 2019, 442ss, spec. nel richiamo al rapporto *Competition policy for the digital era* curato da J. Crémer, Y.A. de Montjoye, H. Schweitzer (COMMISSIONE EUROPEA, 2019), 25ss. Sull'utilizzo di profili per finalità di *dynamic pricing* v. C. LANGHANKE, M. SCHMIDT-KESSEL, Consumer Data as Consideration, 4, Journal of European Consumer and Market Law, 6, 2015, 218ss.

[149] Una delle tecniche principali di aggregazione dei dati, infatti, riguarda proprio tale peculiare fonte di produzione di dati comportamentali e consiste nel sincronizzare i diversi ID identificativi associati

dell'economia digitale, mostrano una rinnovata capacità predittiva imputabile a quel peculiare prodotto informativo dell'industria 4.0 che sono i *behavioral data*, ovvero informazioni sulle preferenze, gli interessi, le attitudini degli utenti ricavate dal monitoraggio del comportamento online degli stessi per mezzo di strumenti di tracciamento tra cui spiccano i *cookies* di profilazione e i dispositivi di *Internet of Things* (IoT)[150]. È proprio nella particolare invasività di questo nuovo patrimonio informativo che si annidano i principali rischi dell'"*interest-based advertising*" e, più in generale del *predictive consumer scoring*[151], primo fra tutti quello della c.d. falsificazione delle preferenze[152].

Questa breve ricognizione empirica delle caratteristiche funzionali dei metadati, rendendo evidenti le ragioni della loro spiccata remunerativitá e centralità nel mercato dei dati, non può che indurre a condividere la posizione di chi ravvisa nel regime di circolazione di questi ultimi, in quanto dati creati dal titolare "in secondo grado", una deviazione dal modello sin qui analizzato verso logiche, stavolta sì, di stampo proprietario[153].

---

da più operatori al medesimo dispositivo (c.d. *cookie syncing*) ovvero associati a più dispositivi (c.d. *cross device graph*). J. BARRETT GLASGOW, *Data Brokers: Should They Be Reviled or Revered?, cit.*, 33-35.

[150] Ivi, 36. Cfr. A. REINALTER, S. VALE, Cookie e consenso dell'utente, in *Giur. It.*, 2020, 79 ss; A. REINALTER, S. VALE, Trattamento dei dati personali. Cookie e consenso dell'utente, in *Giur. It.*, 2020, 1, 79 ss.

[151] Sui rischi che tali operazioni pongono in punto di trasparenza, discriminazione, equità e precisione vedi, fra gli altri, B. SCHERMER, *Risks of Profiling and the Limits of Data Protection Law*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*, Springer, Berlino, 2013, 137ss.

[152] Inteso come la tendenza a manifestare pensieri e preferenze conformi a quelle fatte proprie dal contesto sociale di riferimento, la dimensione digitale e ubiquitaria assunta dalla socialità contemporanea, monitorata (se non controllata) dai gestori delle piattaforme di *social networking*, rende tale pressione valoriale sempre più battente e pericolosa perché suscettibile di condizionare le condotte degli utenti (e quindi della domanda di mercato) in modo sostanzialmente impercettibile in ragione della dilagante assuefazione verso il notorio fenomeno del capitalismo di sorveglianza. V. sul punto le parole T. KURAN, *Private Truths, Public Lies: The Social Consequences of Preference Falsification*, Cambridge (MA), Harvard University Press, 1995, 3ss richiamate da P.M. SCHWARTZ, Internet Privacy and the State, cit., 841, nell'osservare come "*beyond a certain point of intensity, this herd behavior distorts public discourse and then alters both private knowledge ("the understandings that individuals carry in their own heads")'" and private preferences (the preference that one "would express in the absence of social pressures"). At the extreme, a withdrawal of "beliefs from the realm of the thinkable to that of the unthinkable" occurs*. […] *My initial point is merely that the release and suppression of personal data play a powerful though not inevitably salubrious role in formation of social beliefs*." Cfr. S. ZUBOFF, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019, *passim*.

[153] Tesi formulata da V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 49. "Diverso è il caso che i dati siano inventati, artisticamente rappresentati, rielaborati o creati dall'interessato, perché in questo caso potrebbero essere qualificati come opere d'arte o invenzioni, ed avrebbero allora una diversa tutela." G. ALPA, *La "proprietà" dei dati personali*, cit., 27.

La stessa Commissione europea nella Comunicazione "Costruire un'economia dei dati europei" (COM (2017) 9 *final*) del 10 gennaio 2017, internalizzando la sensibilità che la crescita del mercato digitale ha accentuato verso le esigenze della libera circolazione dei dati, ha ammesso la possibilità che "i fabbricanti o fornitori di servizi poss[ano] divenire di fatto "proprietari" dei dati generati dalle loro macchine o processi"[154].

Rinviando al prossimo capitolo ulteriori riflessioni sulle ripercussioni che il riconoscimento di una privativa commerciale sui metadati può produrre sul diritto dell'interessato a una spiegazione significativa della logica seguita nell'assumere decisioni automatizzate nei propri confronti, non rimane che prendere atto dell'inconfigurabilità di un segreto commerciale sul patrimonio informativo raccolto dal titolare e concludere il tentativo di inquadramento dogmatico del suo diritto al trattamento dei dati altrui assumendo una prospettiva negoziale[155].

[154] Sul passaggio dalla dimensione individuale a quella collettiva della privacy legata alla dimensione dell'individuo quale componente di un gruppo sociale si veda meglio *infra sub* Cap. II § 2.5.1. Cfr. S. RODOTÀ, *Tecnologie e diritti*, 19ss.

[155] Un invito ad abbandonare una prospettiva dominicale e guardare al trattamento dei dati personali come fenomeno negoziale è stato formulato, fra gli altri, da RODOTÀ, il quale invitata a focalizzare l'attenzione sulle modalità di appropriazione (e formazione) delle nostre personalità piuttosto che dei nostri dati. ID., *Il mondo nella rete. Quali i diritti, quali i vincoli*, 13 e 33ss. Nello stesso senso ha concluso la dottrina che, negando l'esistenza di un diritto di proprietà (anche intellettuale) sui dati così come dell'opportunità di crearlo, ha sottolineato che "[*n*]*ew property rights in data are not suited to promote better privacy or more innovation or technological advances, but would more likely suffocate free speech, information freedom, science, and technological progress. The rationales for propertizing data are not compelling and are outweighed by rationales for keeping the data "open." No new properly rights need to be created for data*". L. DETERMANN, No One Owns Data, cit., 43. Ancora, affine è la posizione di CIANI nella parte in cui evidenzia come "[*a*]*gainst the backdrop of the ongoing debate on the question of whether or not exclusive rights in digital data should be introduced, relying on contracts seem by far the favorite solution in the political, economic and academic fields*. […] *Even without exclusive rights, firms can retain control over data and determine who is authorised to access it, both through contractual (by imposing obligations, such as penalties in case of unauthorised disclosure) and technical restrictions*." J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., 847-848. Cfr. L.R. PATTERSON, Free Speech, Copyright, and Fair Use, 40 *Vand. L. Rev.*, 1987, 1, 6; J.M. VICTOR, The Eu General Data Protection regulation: Toward a Property Regime for Protecting Data Privacy, cit., 525.

1.6. Il trattamento lecito come fonte di obbligazioni "fiduciarie" sui dati personali altrui

Le riflessioni sin qui condotte circa la natura giuridica del "potere specifico[156]" che il titolare viene ad esercitare sul dato altrui in virtù del suo diritto soggettivo al trattamento dello stesso hanno rivelato il fallimento dell'impostazione ermeneutica volta a inquadrarlo entro il paradigma dello *ius excludendi alios*. In questo senso, le menzionate cause empirico-dogmatiche dell'inadeguatezza del diritto di proprietà, così come della proprietà intellettuale e del segreto commerciale, a fornire il quadro giuridico entro il quale delineare i confini delle prerogative del titolare sul dato altrui, lasciano all'interprete una sola alternativa: guardare alla fattispecie in prospettiva relazionale, o meglio, obbligatoria.

Tale soluzione, ergendo i diritti di credito a paradigma ermeneutico di riferimento, consentirebbe di spostare l'attenzione dal potere di escludere (da parte dell'interessato) a quello di utilizzare il bene per conseguirne un vantaggio (da parte del titolare del trattamento)[157].

Nel riflettere sulla configurabilità di una dinamica negoziale nella circolazione degli attributi della personalità, la dottrina ha tradizionalmente individuato il principale ostacolo ermeneutico nella difficile definizione degli aspetti della titolarità di tali attributi, dell'identificazione dei soggetti coinvolti, dell'oggetto del negozio stesso, nonché della natura giuridica delle dichiarazioni unilaterali di volontà con cui si conferisce il diritto di sfruttamento dello specifico tratto della personalità[158].

Se, tuttavia, con riguardo al diritto soggettivo al trattamento del dato personale altrui le osservazioni sin qui formulate consentono di ritenere sciolti i primi tre nodi

[156] V. S. PUGLIATTI, Beni (voce) (teoria generale), *cit*., §9 nella parte in cui definisce il diritto soggettivo come il "potere specifico attribuito al soggetto come proprio in relazione ad un dato bene giuridico".

[157] Qui, infatti, risiede quella differenza di contenuto che NICOLÒ, *L'adempimento dell'obbligo altrui*, 84 poneva a *discrimen* tra diritti reali e diritti di credito, individuando nel potere di conservare e escludere gli aspetti essenziali dei diritti reali, mentre nel potere di conseguire l'elemento essenziale dei diritti di credito.

[158] V. ZENO-ZENCOVICH, Profili negoziali degli attributi della personalità, cit., *passim*.

interpretativi[159], rimane da affrontare il tema (sinora soltanto accennato[160]) del ruolo e della natura giuridica del consenso dell'interessato. A tal proposito, però, è fin d'ora opportuno precisare che, nella prospettiva del titolare qui assunta, il consenso degrada ad una delle plurime e alternative basi giuridiche per il trattamento dei dati altrui. Esula, quindi, dall'economia della presente trattazione riproporre una esaustiva ricognizione della copiosa dottrina sviluppatasi sul rapporto che tale manifestazione di volontà dell'interessato intrattiene con la sua personalità[161].

Al contrario, prendendo le mosse dalla biforcazione dottrinale tra valenza traslativo-negoziale e autorizzatorio-conformativa del consenso[162], si tenterà di metterne in risalto i tratti funzionali che lo accomunano alle altre condizioni di liceità del trattamento e investigarne le ripercussioni sull'inquadramento dogmatico delle prerogative del titolare.

Se, allo scopo, si sposasse, ad esempio, la tesi del consenso quale atto autorizzatorio con efficacia scriminante di un trattamento dei propri dati che, altrimenti, risulterebbe illecito, si opererebbe un'assimilazione di tale manifestazione di volontà a

[159] Sulla "titolarità" del dato personale altrui quale bene in senso giuridico oggetto del diritto soggettivo al suo trattamento e conseguentemente, della definizione della posizione attiva del titolare come speculare e complementare a quella dell'interessato, si vedano le riflessioni compiute, rispettivamente, *supra sub* § 1.3. Quanto invece alla migliore definizione dell'oggetto del diritto e della natura giuridica del potere del titolare sullo stesso si vedano le osservazioni (critiche) sul diritto di proprietà o proprietà intellettuale sul singolo dato altrui svolte *supra sub* §1.4. e 1.5.

[160] Sulla funzione di reificazione del consenso si veda quanto già detto supra sub §1.3 e quanto ancora si dirà *infra* in questo paragrafo.

[161] Cfr. L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, cit., 58ss; E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy*, in ID. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., 28ss; T. Pasquino, Identità digitale della persona, diritto all'immagine e reputazione, ivi, 99ss; D. MESSINETTI, Personalità (diritti della) (voce), cit., § 1; G. BAVETTA, Identità (diritto alla), *Enc. dir*., XIX, Milano, Giuffré, 1970, 953ss.

[162] In altri termini, la dottrina si è divisa tra un approccio liberale tendente a privilegiare la funzione negoziale del consenso e una posizione interpretativa più "garantista" che, muovendo dall'accezione del dato personale come espressione e parte della personalità dell'interessato, propende per la tesi del consenso quale autorizzazione, ricondotta quindi alla funzione scriminante del consenso dell'avente diritto. Ci si avvicina in questo modo alla fattispecie degli atti disposizione del proprio corpo il cui consenso non può essere configurato come "atto di autonomia contrattuale regolato dal quarto libro del codice, ma è atto unilaterale sempre revocabile" (F. GALGANO, *Diritto privato*, XVIII ed., Padova, Cedam, 2019, 261ss) e, di conseguenza, inidoneo a creare in capo a chi lo presta obbligazioni suscettibili di esecuzione forzata. Condivide la tesi per cui il consenso disciplinato dalla legge n.675/1996 è stato concepito quale esimente per escludere l'illiceità del trattamento, privo di qualsivoglia funzione negoziale V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 29. Vedi anche S. SICA, Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica, *Riv. dir. civ*., 2001, 621 ss. Cfr. G. RESTA, V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, cit., *passim*; I.A. CAGGIANO, Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali, *Osservatorio del diritto civile e commerciale*, 1, 2018, 67ss.

quelle facoltà di (limitata) disposizione dei propri diritti fondamentali che De Cupis inquadrava nelle facoltà di consentirne lesioni[163]. Una siffatta impostazione ermeneutica, per quanto più coerente alla natura extracontrattuale dei rimedi apprestati dal GDPR per eventuali violazioni[164], guarda al consenso solo dal punto di vista dell'interessato e, di conseguenza, mal si concilia con le esigenze di coerenza sistematica raffigurate in apertura al paragrafo. Ciò in quanto, se si muove dal presupposto dell'intrinseca antigiuridicità delle operazioni di trattamento dei dati si nega *ab origine* la meritevolezza dell'interesse perseguito dal titolare e, *a fortiori*, la stessa configurabilità di un diritto al trattamento dei dati altrui[165].

L'impostazione squisitamente personalistica non convince neppure associando la natura autorizzatoria del consenso ad una diversa funzione c.d. normativa o conformativa del consenso, riguardato come manifestazione di volontà con cui l'interessato influirebbe sull'assetto dell'operazione di trattamento dei propri dati[166]. Anche in questo caso, infatti, guardando alla fattispecie dalla prospettiva del titolare del trattamento e della sua situazione giuridica soggettiva attiva, non è ravvisabile alcuna disposizione del GDPR che attribuisce all'interessato il diritto di incidere attivamente sulle finalità e modalità del trattamento così come predeterminate e predisposte dal titolare. Queste ultime, peraltro, pur dovendo essere comunicate all'interessato nell'assolvimento degli obblighi informativi del titolare, non devono neppure essere necessariamente "approvate" dal primo, il cui consenso (*rectius* assenso) diviene del tutto superfluo ove sussista una diversa condizione di liceità del trattamento effettuato sui suoi dati[167].

---

[163] A. DE CUPIS, *I diritti della personalità*, Milano, Giuffré, 1982, 96ss.

[164] G. ALPA, *La "proprietà" dei dati personali*, cit., 23.

[165] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 19-20 spec. nt 19 ove richiama l'affine posizione espressa da S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati*, Milano, Giuffré, 2006, 1021ss.

[166] Cfr. D. MESSINETTI, Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali, cit., 352ss; V. RICCIUTO, *L'economia della privacy. Circolazione dei dati personali e mercato*, in E. PICOZZA, V. RICCIUTO, *Diritto dell'economia*, Giappichelli Editore, Torino, 2013, 311 ss; F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 138ss.

[167] In senso analogo si è espresso BRAVO, per cui "[i]l meccanismo delineato in materia di protezione dei dati personali non prevede che l'interessato concorra a determinare le regole e le modalità del trattamento, che in realtà vengono rimesse alla sola valutazione del titolare. Ciò si ricava con evidenza non solo dal tenore delle disposizioni relative al titolare del trattamento, ma anche dalle logiche di funzionamento dei trattamenti di dati personali: il titolare, quando pone in essere un trattamento di dati personali, stabilisce finalità, modalità e caratteristiche di trattamento uniche – o comunque omogenee- per i dati personali da trattare, i quali di riferiranno non ad un solo interessato, ma ad una serie indefinita o

Spostando invece l'attenzione sulla tesi del consenso quale atto dispositivo con cui l'interessato trasferisce al titolare diritti e facoltà sui propri dati[168] è possibile osservare come, pur offrendo l'indubbio pregio di internalizzare la dimensione patrimoniale del dato quale "possibile oggetto della prestazione"[169], tale impostazione trascuri la circostanza della assoluta mancanza di corrispondenza tra le facoltà di accesso, cancellazione, portabilità e, più in generale, controllo, che l'interessato può esercitare in quanto estrinsecazione legislativa del suo diritto alla protezione dei dati personali, e le facoltà di determinare finalità (anche di lucro) e mezzi del trattamento che il GDPR esplicitamente (seppure indirettamente) riconosce e attribuisce al titolare e che, come visto in precedenza, sono qui riguardate come il contenuto del diverso diritto soggettivo al trattamento dei dati altrui[170]. Peraltro, ove anche si volesse guardare al rapporto che l'interessato intrattiene con i propri dati personali come una forma di trattamento "effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico", il considerando 18 GDPR esclude espressamente una tale fattispecie dall'ambito materiale di applicazione del Regolamento, rendendo in tal modo anche in quest'ottica impossibile riconoscere in capo agli interessati poteri analoghi a

molteplice di interessati: il titolare non andrà a determinare le modalità e le caratteristiche del trattamento sulla base di regole determinate con il concorso di ciascun interessato, ma si preoccuperà di soddisfare quelle condizioni di liceità del trattamento che – tramite la raccolta di un consenso "adesivo" o la soddisfazione di altri presupposti legittimanti alternativi al consenso dell'interessato- porteranno a far considerare lecita l'attività di trattamento con riguardo ai dati personali di ciascun interessato, assoggettati uniformemente ai criteri, alle modalità ed alle finalità approntate per tutta la serie di dati raccolti e trattati. ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 17, spec. nt. 19.

[168] In questo senso si è espresso, fra gli altri, RICCIUTO, per il quale "[i]l consenso dell'interessato, invece, è coerentemente concepito dal legislatore comunitario come consenso negoziale, manifestazione di volontà in ordine alla circolazione dei dati personali. La peculiarità del bene e del fenomeno della sua circolazione giustifica, innegabilmente, alcune deviazioni dal modello generale del contratto, ma non colloca il trasferimento dei dati personali fuori dalla dimensione patrimoniale e, dunque, dalla dimensione contrattuale." ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 56. Cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., 996ss.

[169] A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, Napoli, Edizioni Scientifiche italiane, 2017, 68.

[170] Come condivisibilmente osservato da BRAVO in tal senso "il titolare del trattamento, a seguito del "consenso-assenso" dell'interessato, non va ad esercitare poteri, facoltà o diritti originariamente spettanti all'interessato medesimo". Meno condivisibile, invece, la conclusione che ne viene tratta per cui la funzione del consenso sarebbe, invece, quella di "rimuove[re] un impedimento all'esercizio del diritto, di un potere e di una facoltà che già fanno capo al titolare del trattamento (in forza dell'autonomia privata e dei diritti di libertà economica […]." ID., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 117, spec. nt. 126. Cfr. E. LUCCHINI GUASTALLA, Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori, *Contratto e impresa*, 1, 2018, 111-116; S. PATTI, Il consenso dell'interessato al trattamento dei dati personali, *Riv. dir. civ.*, 2, 1999, 455 ss.

quelli che il disposto normativo attribuisce ai titolari di trattamenti svolti in "connessione con un'attività commerciale o professionale" [171].

Tale impostazione negoziale, inoltre, opera una razionalizzazione giuridica della fattispecie del trattamento dei dati altrui che, ai fini dell'analisi qui condotta, risulta insoddisfacente in quanto inevitabilmente parziale. L'efficacia traslativa per tal via ascritta al consenso, infatti, non è in ogni caso ravvisabile nelle altre condizioni (oggettive) di liceità del trattamento in quanto prive di qualsivoglia tratto negoziale e, anzi, produttive di effetti subordinati a valutazioni talvolta rimesse allo stesso titolare da parte del legislatore[172].

Obiezione, quest'ultima, avallata dagli stessi fautori del c.d. schema "servizi contro dati[173]" che, pur declinando la dimensione negoziale del consenso in termini più dispositivi (dei dati) che traslativi (delle facoltà sugli stessi)[174], ammettono la configurabilità di una vera e propria obbligazione avente ad oggetto la cessione di dati personali (in cui la prestazione dell'interessato si identificherebbe nel consenso al trattamento) soltanto ove la liceità del trattamento in questione non sia basata su un'altra

[171] GDPR, Considerando 18. Per una critica alla possibilità di interpretare il regime di circolazione dei dati personali (così come disciplinato dalla previgente Direttiva) in senso di atti dispositivi o traslativi di un diritto v. S. PATTI, *Consenso, sub art. 23*, cit., *passim*.

[172] È questo, ad esempio, il caso di trattamenti fondati su esigenze di salvaguardia di interessi vitali dell'interessato ex artt. 6(1)(d) e 9(2)(c) ovvero di perseguimento di legittimi interessi *ex* art. 6(1)(f) GDPR. Nello stesso senso si veda la posizione di chi ha osservato come "[l]'ordinamento giuridico, in altre parole, ammette che la circolazione dei dati […] sia realizzata dal titolare del trattamento per finalità determinate che siano rispondenti ad un interesse proprio (del titolare del trattamento) e dell'interessato medesimo, anche al di fuori di logiche contrattuali". F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 81-82.

[173] Tale dottrina argomenta l'"ammissibilità dello schema "servizi contro dati"" osservando come il dettato della Carta di Nizza, nell'omettere una reiterazione dell'espresso divieto di monetizzazione e mercificazione delle parti del corpo con riguardo al dato personale, abbia indirettamente escluso la necessarietà legislativa, prima ancora che dogmatica, di una de-patrimonializzazione dei dati. Ne conseguirebbe, sostengono gli Autori, "che la «monetizzazione» dei dati personali non abbia in sé nulla di disdicevole né di giuridicamente «sospetto», purché però il consenso in oggetto rappresenti una effettiva espressione della «autodeterminazione informativa»". Così G. RESTA, V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, cit., 428. Cfr. G. RESTA, Autonomia contrattuale e diritti della personalità nel diritto dell'UE (voce), *Dig. disc. priv*., Sez. civ., Torino, 2013, 92ss; V. ZENO ZENCOVICH, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, cit., 120ss.

[174] Per riflessioni sui rapporti in cui "un soggetto fornisce (o si impegna a fornire) ad un altro soggetto, dietro corrispettivo, una informazione" v. V. ZENO-ZENCOVICH, Cosa (voce), *cit*., §13. Cfr. G. OPPO, *Sul consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffré, 1999. Sulla contestualizzazione digitale dello scambio dati-servizi online secondo lo schema del c.d. "*disclosure as by-product*" si vedano le riflessioni di G. MALGIERI, Pricing Privacy, cit., 294.

delle basi giuridiche di cui agli artt. 6 e 9 GDPR che, rendendo superfluo il consenso, farebbero quindi venire meno l'oggetto della prestazione[175].

Impasse interpretativa, questa, apparentemente superata dalla più recente dottrina che, accogliendo l'impostazione fatta propria dal legislatore eurounitario nella proposta di direttiva sulla fornitura di servizi digitali, individua nel dato stesso l'oggetto di quella che, a seguito della prestazione del consenso, assume i connotati di una "controprestazione non pecuniaria" [176]. In particolare, De Franceschi, sviluppando la tesi attraverso la promozione di una più ampia interpretazione della nozione di pagamento[177], idonea a ricomprendervi anche atti solutori diversi da quelli aventi ad oggetto una prestazione di dare, ingloba il consenso nella più ampia manifestazione di volontà volta alla conclusione di un contratto "a titolo oneroso" di fornitura di contenuti digitali. In questo senso, sostiene l'Autore, le rappresentazioni di gratuità dell'affare operate dal titolare del trattamento in sede di conclusione in via elettronica del contratto, risulterebbero ingannevoli e, quindi, censurabili ai sensi dell'articolo 51 cod. cons. nella

[175] In particolare, nelle parole dell'Autore: "[i]l consenso al trattamento dei dati personali fornito dal titolare degli stessi rappresenta […] la base giuridica del rapporto obbligatorio "dati personali verso controprestazione" ed è pertanto il fulcro dell'obbligo sottostante" nonché "parte costitutiva della controprestazione" che, di conseguenza, viene a configurarsi come atipica. In quest'ottica il contratto per l'utilizzo di social network, ad esempio, verrebbe a configurarsi come un contratto di durata avente ad oggetto l'autorizzazione al trattamento dei dati personali. Così A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto,* cit., 72, 75-76. Ad analoghi approdi conduce la strada ermeneutica parallelamente tracciata da MESSINETTI che, seppure con riguardo alla non del tutto identica fattispecie dello sfruttamento economico della propria immagine, individua l'oggetto dell'atto dispositivo con cui l'interessato ne autorizza unilateralmente la pubblicazione nel "facere necessario a dar vita al bene" e quindi, nel caso del trattamento dei dati altrui, in un consenso dell'interessato inteso come "*quid* preliminare e necessario […] che funge da presupposto di legittimazione allo svolgimento di quella attività." D. MESSINETTI, Personalità (diritti della) (voce), cit., § 31.b. Cfr. G. RESTA, Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali, 7, *Riv. crit. dir. priv*., 2000, 299 ss; S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., 994 ss.

[176] G. ALPA, *La "proprietà" dei dati personali*, cit., 12. Cfr. G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, in R. SACCO (diretto da), *Trattato di diritto civile*, Vol. I, II ed., Torino, Utet, 2019, 463ss; V. ZENO ZENCOVICH, Personalità (diritti della) (voce), cit., *passim*; G. SIMEONE, Mercato unico digitale (voce), Enciclopedia Treccani online, 2016 disponibile all'indirizzo www.treccani.it/enciclopedia/mercato-unico-digitale; M. LEHMANN, *A European Market for Digital Goods*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The implications of the Digital Revolution*, Cambridge, Intersentia, 2016, 115 ss; V. JANECEK, G. MALGIERI, Data Extra Commercium, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Data as Counter-Performance—Contract Law 2.0?*, Hart Publishing/Nomos, 2019, 4 ss; A. ADDANTE, La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali, *Giustizia civile*, 4, 2020, 889 ss; C. CAMARDI, Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali, in *Giustizia civile*, 2019, 499 ss; V. CUOCCI, Fornitura di contenuti digitali e controprestazione non pecuniaria: luci e ombre sulla tutela del consumatore nella prospettiva del diritto contrattuale europeo, in F. Di Ciommo, O. Troiano (a cura di), Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido, Studi in onore di Roberto Pardolesi, Piacenza, 2018, 269 ss.

[177] Cfr. G. CIAN, Pagamento (voce), *Dig. Disc. Priv*., Sez. civ., XIII, Torino, 1995, 234; A. DI MAJO, *Delle obbligazioni in generale*. *Art. 1173-1176*, Bologna, Zanichelli, 1988, 121ss.

parte in cui impone al professionista di concentrare l'attenzione del consumatore sugli elementi essenziali del contratto "in modo chiaro ed evidente", inclusa quindi l'onerosità della controprestazione richiesta, prima che quest'ultimo inoltri l'ordine[178].

Tale soluzione, tuttavia, seppure astrattamente ricavabile dalla formulazione adottata dal legislatore eurounitario in sede di proposta della Direttiva sulla fornitura di contenuti digitali, sembrerebbe essere in aperto contrasto con il dettato normativo confluito nella versione finale della stessa. Nel disciplinare la fattispecie dello scambio tra dati personali e servizi, infatti, il legislatore eurounitario ha abbandonato l'assimilazione del consenso all'accesso ai propri dati personali ad una "controprestazione non pecuniaria[179]" originariamente contenuta nella proposta di direttiva (UE) 2019/770, sostituendola con la puntualizzazione per cui siffatto modello commerciale non implica in alcun modo l'assimilazione dei dati personali ad una merce[180].

---

[178] A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, cit., 91. Cfr. G. VERSACI, La contrattualizzazione dei dati personali dei consumatori, Napoli, ESI, 2020, *passim*. Per una riflessione critica dell'incertezza derivante dalla difformità delle soluzioni adottate dai vari Stati membri nel disciplinare le conseguenze della violazione dei richiamati obblighi formali *ex* art. 8 par. 2 dir. 2011/83/UE v. A. DE FRANCESCHI, The EU Digital Single Market Strategy in Light of the Consumer Rights Directive, 4, *Journal of European Consumer and Market Law*, 4, 2015, 144ss.

[179] V. i considerando 13,14 e 15, nonché l'articolo 6 co.2 lett.a della Proposta di Direttiva del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale (COM/2015/0634 final). Cfr. F. BRAVO, Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto, 1, *Contratto e impres*a, 2019, 34 ss; R. SCHULZE, *Supply of Digital Content. A New Challenge for European Contract Law*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The implications of the Digital Revolution*, cit., 131ss; W. KERBER, *Rights on Data: The EU Communication 'Building a European Data Economy' from and Economic Perspective*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Oxford, Hart Publishing, 2017, 109ss.

[180] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, GUUE L.136/1 [d'ora in avanti Direttiva sulla fornitura di contenuto digitale e di servizi digitali], Considerando 24. Il Considerando 38, dal canto suo, ribadisce inoltre come "qualsiasi trattamento di dati personali in relazione a contratti rientranti nell'ambito di applicazione della presente direttiva è lecito solo se è conforme alle disposizioni del regolamento (UE) 2016/679 relativo ai fondamenti giuridici per il trattamento dei dati personali" e, ancora, come "gli elementi che determinano un difetto di conformità rispetto ai requisiti di cui al regolamento (UE) 2016/679 […] [possano costituire] un difetto di conformità del contenuto digitale o del servizio digitale rispetto ai requisiti di conformità soggettivi od oggettivi di cui alla presente Direttiva. Un esempio potrebbe essere rappresentato dai casi in cui un operatore economico assum[a] in maniera esplicita un obbligo contrattuale […] connesso agli obblighi dell'operatore economico di cui al regolamento (UE) 2016/679. In tal caso, l'impegno contrattuale [potrebbe] essere inserito tra i requisiti di conformità soggettivi. Un secondo esempio potrebbe essere rappresentato dai casi in cui la mancata conformità agli obblighi di cui al Regolamento (UE) 2016/679 potrebbe allo stesso tempo rendere il contenuto digitale o il servizio digitale inadeguato alla sua finalità prevista e costituire pertanto un difetto di conformità ai requisiti di conformità oggettivi, che prevedono che il contenuto digitale o il servizio digitale sia adeguato alle finalità per le quali è abitualmente utilizzato un contenuto digitale o un servizio digitale dello stesso tipo." (Considerando 48). Cfr. G. RESTA, *Le persone fisiche e i diritti della personalità*, cit., 547ss.

Tale precisazione legislativa si è resa necessaria in quanto, come già osservato da Guido Alpa richiamando l'analoga posizione assunta dallo *European Data Protection Supervisor*, qualificare il consenso prestato come controprestazione avrebbe implicato l'assimilazione dogmatica dello scambio ad una cessione di dati e non ad una condizione di liceità del servizio[181].

Ne discende che, fin quando l'influenza sistematica esercitata dall'articolo 16 TFUE (e dall'art. 8 della Carta di Nizza) continuerà ad incidere sulla nozione di dato personale, impendendone l'assimilazione a "bene" oggetto di "controprestazione non pecuniaria", risulta giuridicamente insostenibile[182], per quanto astrattamente condivisibile, censurare la condotta del professionista/titolare del trattamento che abbia omesso di chiaramente rappresentare come onerosa un'operazione che il legislatore eurounitario espressamente vieta di configurare come tale. In mancanza di un *revirement* normativo risulta quindi poco percorribile la tesi del dato personale (e del consenso al suo trattamento) quale controprestazione non pecuniaria[183].

Non è però questa la conclusione raggiunta dalla prima sezione del T.A.R. Lazio nel decidere il ricorso presentato da Facebook Inc. avverso il provvedimento con cui l'Autorità Garante della Concorrenza e del Mercato aveva, tra l'altro, censurato in quanto "ingannevole" ai sensi degli articoli 21 e 22 D.Lgs. n.206/2005 l'informativa che, fino al 15 aprile 2018, l'utente in procinto di registrarsi sulla piattaforma riceveva circa il carattere squisitamente "gratuito" del servizio ivi offerto. A fronte del difetto assoluto di attribuzione dell'AGCM eccepito dal ricorrente, infatti, il T.A.R. ha ritenuto priva di pregio l'argomentazione per cui l'assenza di un corrispettivo patrimoniale escludesse la

[181] Cfr. G. ALPA, *La "proprietà" dei dati personali*, cit., 26; *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* (EUROPEAN DATA PROTECTION SUPERVISOR, 14 marzo 2017).

[182] A tal riguardo, efficace è il richiamo che DURST fa alla nozione di "bilanciamento ineguale" (già sviluppata da RODOTÀ) nel notare come il legislatore euronitario abbia mostrato con il GDPR un *favor* per la tutela della protezione dei dati come diritto fondamentale, accentando parziali compressioni delle esigenze del mercato dei dati. Così L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, cit., 60, spec. nt. 43 ove richiama le parole di S. RODOTÀ, in occasione del convegno "Governance di Internet ed efficienza delle regole: verso il nuovo regolamento europeo sulla privacy" organizzato dall'Accademia Italiana del Codice di Internet, del 13 novembre 2014.

[183] Di conseguenza, parimenti insostenibile, *de iure condito*, la conseguenza trattane della non vincolatività di contratti di fornitura di contenuti digitali conclusi per via elettronica e dietro prestazione del consenso al trattamento dei dati personali del consumatore in virtù del divieto di forniture non richieste di cui agli artt.20, co.5 e 26, co.1 lett. f cod. cons., ovvero della possibilità di ravvisarvi gli estremi di una pratica commerciale scorretta consistente nella ingannevole rappresentazione di gratuità del bene o servizio fornito ai sensi dell'articolo 23, co.1, lett. v cod. cons. sviluppata da A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, cit., 101-102.

configurabilità *ab origine* di una pratica commerciale scorretta e, di conseguenza, la competenza dell'Autorità. Ciò in quanto, nelle parole dei giudici amministrativi, "tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto.[184]" Conclusioni, queste ultime, peraltro recentemente avallate anche dal Consiglio di Stato il quale, tuttavia, sembrerebbe essersi maggiormente concentrato sul carattere autonomo ma complementare dei corpi normativi costituiti dal codice del consumo e dal GDPR che non sulla riconducibilità o meno dei dati alla sfera delle *res extra commercium*[185].

Tuttavia, anche a voler ignorare (*rectius* abbattere) il pilastro dogmatico della gratuità dello scambio eretto dall'articolo 16 TFUE[186], si incapperebbe, ancora una volta, in un'intrinseca contraddizione giuridica nella misura in cui, se riconoscere natura negoziale al consenso significa identificarlo con l'oggetto di una (contro)prestazione volta a ottenere l'accesso a beni o servizi, ovvero ad accedervi a prezzo ridotto, siffatta manifestazione di volontà non potrà che considerarsi ontologicamente incompatibile con la disciplina del GDPR nella parte in cui impedisce di considerare libero, e quindi valido, il consenso prestato ad un trattamento di dati che, sebbene non necessario all'esecuzione

[184] Peraltro, a confutazione del carattere asseritamente imprevedibile di tale interpretazione "estensiva" delle norme sanzionatorie in materia di pratiche commerciali scorrette, la Corte ha richiamato, fra gli altri, la presa d'atto del "valore economico *de facto*" assunto dai dati personali degli utenti, nonché l'assimilazione, operata dalla stessa AGCM in un altro provvedimento dell'11 maggio 2017 con cui si è sanzionato l'uso commerciale e per finalità di *marketing* dei dati degli utenti ad un rapporto di consumo tra professionista ed utente ai fini dell'applicabilità della disciplina sulle pratiche commerciali scorrette, proprio in ragione del valore economico assunto da tale patrimonio informativo. T.A.R. Lazio Roma Sez. I, Sent., (ud. 18-12-2019) 10-01-2020, n. 261, §§ 6-7. Cfr. C. SOLINAS, Trattamento dei dati personali e pratiche commerciali scorrette, in *Giur. It.*, 2, 320 ss.

[185] In particolare, ad avviso della Corte "seppure si volesse aderire alla tesi della odierna parte appellante secondo la quale il dato personale costituisce *una res extra commercium*, la patrimonializzazione del dato personale, che nel caso di specie avviene inconsapevolmente (ad avviso dell'Autorità nel momento in cui accusa una informazione ingannevole nell'esercizio della pratica in questione), costituisce il frutto dell'intervento delle società attraverso la messa a disposizione del dato – e della profilazione dell'utente – a fini commerciali". Così Cons. Stato, sentenza 29 marzo 2021, n. 2631.

[186] Il Garante europeo per la protezione dei dati mette in guardia circa la configurabilità di una fattispecie in cui l'interessato presti il consenso al trattamento dei propri dati come controprestazione non pecuniaria. Nel suo parere n.4/2017, infatti, lo EDPS mette in guardia circa l'utilizzo di un linguaggio tale da suggerire l'idea per cui sia possibile pagare con i propri dati allo stesso modo in cui si paga con la moneta. Ciò in quanto, la natura fondamentale del diritto alla protezione dei dati personali impedisce qualsivoglia assimilazione del dato ad una "*mere commodity*". In questo senso, si riferisce al GDPR come ad uno "statuto della *Data economy*" M. MAGLIO, *Il regolamento europeo 2016/679 in materia di dati personali: inquadramento generale e prospettive di sviluppo*, in M. MAGLIO, M. POLINI, N. TILLI (a cura di), *Manuale di diritto alla protezione dei dati personali*, II ed., Santarcangelo di Romagna, Maggioli Editore, 2019.

del contratto, ne diventa presupposto[187]. Delle due l'una: o il consenso non è una controprestazione e quindi colui che lo presta non può ottenere vantaggi in caso di prestazione (come l'accesso gratuito a beni o servizi) né svantaggi in caso di revoca (come la risoluzione contratto); oppure è una controprestazione e quindi il titolare/professionista potrà negare l'accesso al bene o servizio in mancanza del previo consenso al trattamento dei propri dati da parte dell'aspirante utente, ovvero risolvere il contratto in caso di revoca dello stesso[188].

Sull'ambiguità della posizione apparentemente assunta dalla stessa Cassazione sul punto si ritornerà nel prossimo capitolo. Tuttavia, ai fini della conclusione dell'*excursus* dottrinale sin qui ripercorso, e per tutte le ragioni sin qui esposte, è possibile concludere che, allo stato dell'arte, l'unica qualificazione suscettibile di accomunare il consenso alle altre condizioni di liceità *ex* artt. 6 e 9 GDPR è quella di presupposto predefinito di "valutazione in ordine alla "meritevolezza" dell'interesse perseguito dal titolare e al bilanciamento con gli interessi, i diritti e le libertà che fanno capo all'interessato medesimo.[189]" A differenza di quanto concluso dalla dottrina richiamata, però, tali presupposti non sembrerebbero tanto *rimuovere* un ostacolo all'esercizio del diritto al trattamento dei dati altrui[190], quanto *creare*, attraverso il già descritto processo di reificazione dell'informazione personale contenuta nel datore[191], il bene giuridico su cui può cadere il diritto soggettivo del titolare.

Ne consegue che la fattispecie "trattamento lecito dei dati altrui", integrata per effetto del venire ad esistenza di uno dei fattori oggettivi o, nel caso del consenso,

[187] Come noto, infatti, il considerando 43 GDPR puntualizza che "[s]i presume che il consenso non sia stato liberamente espresso […] se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione." Cfr. A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, cit., 74. In senso analogo G. MALGIERI, Pricing Privacy, cit., 9 ove discute dell'incompatibilità di un eventuale modello di c.c. scelta attiva tra la prestazione del consenso al trattamento dei propri dati e il pagamento del prezzo monetario del servizio con il requisito della libertà (*rectius* non condizionalità) del consenso di cui all'articolo 7 GDPR.

[188] Sul punto si vedano le puntuali riflessioni condotte da DE FRANCESCHI in punto di adattamento della disciplina delle obbligazioni e dei contratti a fattispecie caratterizzate dallo scambio di bene/servizio contro dato personale ID., *La circolazione dei dati tra privacy e contratto*, cit., 110ss.

[189] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 116-117.

[190] Ibid.

[191] Sul punto si veda quanto già argomentato *supra sub* §1.4.

soggettivi, a cui il GDPR ha subordinato la rilevanza giuridica dell'interesse perseguito dal titolare, costituisce un fatto giuridico fonte di obbligazioni *ex* art.1173 c.c.[192].

Esclusa, però, per le ragioni già descritte, la natura negoziale del rapporto obbligatorio che il titolare viene ad instaurare con l'interessato per effetto dell'inizio di un'attività di trattamento lecito dei suoi dati personali (tra l'altro, come visto, astrattamente -e problematicamente- configurabile solo in caso di utilizzo della base giuridica del consenso), tale fatto giuridico sembrerebbe sì produttivo di obbligazioni, ma solo in capo al titolare. Emblematica in questo senso la previsione per cui, ad esempio, l'interessato ha il diritto di ottenere la rettifica dei dati inesatti che lo riguardano ma nessun obbligo di fornire dati corretti[193]. Ancora, e a differenza di quanto sostenuto sul punto dalla dottrina richiamata[194], se in capo al titolare è esplicitamente posto l'obbligo di "agevola[re] l'esercizio [di alcuni] dei diritti dell'interessato[195]", nessuna disposizione impone all'interessato di astenersi dall'ostacolare il trattamento dei propri dati da parte di terzi (ad esempio attraverso l'esercizio dei diritti di opposizione, cancellazione e portabilità), né tantomeno di agevolarne il processo o la riuscita.

Al contrario, le obbligazioni che il fatto giuridico del trattamento lecito sembrerebbe far sorgere in capo al titolare, assieme al suo diritto a trattare i dati altrui, si colorano di un peculiare "dovere di cura" degli interessi di protezione dei dati degli interessati, estrinsecati nei vari doveri e limiti posti dal GDPR all'attività di trattamento, e che pongono il titolare in una posizione affine a quella dei cc.dd. "fiduciari informativi[196]" teorizzati da parte della dottrina statunitense e definiti come "*a person or*

---

[192] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 97-99, 104, 107.

[193] GDPR, Articolo 16.

[194] F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 132 il quale ritiene esistenti, in capo all'interessato, obblighi di astensione dal porre in essere atti impeditivi o turbativi del diritto del titolare del trattamento dei propri dati, asseritamente ravvisabili, ad esempio, nella possibilità di esercitare il diritto alla portabilità dei dati nel solo caso in cui non sussista altra base giuridica al di fuori del previo consenso prestato per il trattamento, ovvero nelle altre limitazioni individuate in sede di definizione dei presupposti per l'esercizio dei diritti di opposizione e cancellazione.

[195] Articolo 12 par.2 GDPR.

[196] L'espressione "*information fiduciaries*" è stata coniata da K.C. LAUDON, Markets and Privacy, International Conference on Information Systems, 1993, 65ss, ma solo dal 2014 è stata ripresa e assurta ad epicento delle teorizzazioni di BALKIN, poi a loro volta condivise da buona parte della dottrina ben rappresentata da F. PASQUALE, Lecture, Response: Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society, 78, *Ohio St. L.J.*, 2017, 1243ss. Per una critica delle conseguenze della teoria dei fiduciari informativi sul *free speech*, specialmente ove estesa a peculiari categorie di titolari del trattamento (come, ad esempio, Netflix), si veda J.R. BAMBAUER, The Relationships Between Speech and Conduct, 49, *U.C. Davis L. Rev*., 2016, 1941, 1949ss.

business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.[197]"

In particolare, dopo il forte intervento regolamentare sul mercato operato nel contesto del *New Deal* e della conseguente evoluzione del c.d. "*right to free labor*" nel "*right of freedom to contract*", la tutela del Primo emendamento è assurta a nuovo principale strumento di contrasto agli interventi legislativi sul mercato delle informazioni. Negli Stati Uniti, infatti, lo sfruttamento economico dei dati personali non solo non viene ad essere limitato da concezioni personalistiche del patrimonio informativo individuale[198], ma assurge ad autonomo oggetto di tutela in quanto declinazione di quel c.d. *commercial speech* che, definito come un "*market behavior that attempts to alter public culture to facilitate itself*"[199], gode di una parziale protezione del Primo emendamento, temperata dalla sua natura ibrida per cui, pur essendo volto a plasmare l'opinione pubblica, non contribuisce al "*public discourse*"[200].

È in questo contesto che Balkin ha teorizzato la figura degli *information fiduciaries* per dimostrare come le esigenze di protezione dei dati possano conciliarsi con le contrapposte esigenze di raccolta e trattamento degli stessi sottese al mercato dei dati

[197] Ancora, continua l'Autore, "*a fiduciary is one who has special obligations of loyalty and trustworthiness toward another person. The fiduciary must take care to act in the interests of the other person, who is sometimes called the principal, the beneficiary, or the client. The client puts their trust or confidence in the fiduciary, and the fiduciary has a duty not to betray that trust or confidence. Fiduciaries often perform professional services or else manage money or property for their principals, beneficiaries, or clients. In almost every case, however, fiduciaries also handle sensitive personal information. That is because, at their core, fiduciary relationships are relationships of trust and confidence that involve the use and exchange of information*." J.M. BALKIN, Information Fiduciaries and the First Amendment, 49, *U.C. Davis Law Review*, 2016, 1183, 1207, 1209. Cfr. D.A. DEMOTT, Beyond Metaphor: An Analysis of Fiduciary Obligation, *Duke LJ*, 1988, 879, 882.

[198] Per ulteriori e più ampi approfondimenti della disciplina apprestata dall'ordinamento statunitense in punto di protezione dei dati personali si veda *infra sub* Cap. III, spec. §3.9.

[199] In particolare, il *commercial speech* è riguardato come una forma di comportamento di mercato la cui funzione sociale è indurre le persone ad acquistare beni e servizi. Tuttavia, nota l'Autore, "*unlike the speech involved in bargaining over contracts, commercial speech actively tries to reshape popular culture in order to sell products and services. It does so by providing information, ideas, images, and opinions to the general public, attempting to reshape people's self-image, beliefs and desires*." Così J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1185-1186 e 1213. Cfr. ID., Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79, *N.Y.U. L. Rev*., 2004, 1, 26. Per la tesi che concepisce il *commercial speech* come strumentale alla salvaguardia della disseminazione di messaggi commerciali non in quanto diritto di "espressione" degli inserzionisti, ma in quanto diritto dei consumatori a ricevere tali informazioni si veda R. POST, A. SHANOR, Adam Smith's First Amendment, 128, *Harv. L. Rev. F*., 2015, 165, 172.

[200] Più specificatamente, per *public discourse* si intende una "*critical interaction* […] *within which public opinion, and hence democratic policy, may be formed*." R.C. POST, The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell, 103, *Harv. L. Rev*., 1990, 601, 637ss.

e tutelate dal Primo emendamento come forma di *commercial speech*[201]. In particolare, l'obiettivo dell'Autore è quello di spostare l'accento dalla tipologia di informazioni coinvolte, alla tipologia di relazioni instaurate, mettendo in luce come la peculiarità dei poteri che le grandi imprese digitali vengono ad esercitare sugli interessati per effetto del trattamento dei loro dati personali determini la nascita di uno speciale dovere di cura degli interessi della controparte "debole" del rapporto, giustificando così un più intenso intervento del legislatore a tutela della stessa, senza che ciò possa configurare una violazione del Primo emendamento[202].

In quest'ottica, la raccolta e distribuzione sul mercato dei dati personali assurge ad attività protetta, come peraltro ben espresso nel caso *Sorrell v. IMS Health Inc*.[203] in cui la Corte Suprema ha ritenuto incostituzionale la legge con cui lo Stato del Vermont aveva fissato il divieto dei farmacisti di vendere le informazioni relative alle prescrizioni mediche alle compagnie farmaceutiche che le utilizzavano per finalità di marketing. Il legislatore statale riteneva che tale prassi avrebbe finito per tradursi in una indebita manipolazione delle tendenze prescrittive dei medici verso la scelta di farmaci più costosi. Dal canto suo, invece, il giudice Kennedy, nello scrivere per la maggioranza, ritenne che siffatto intervento legislativo, limitando la circolazione di una specifica categoria di informazioni, provenienti da una specifica categoria di soggetti e utilizzate per finalità di *marketing*, confliggesse con la protezione accordata dal Primo emendamento alla libera circolazione di informazioni nella misura in cui "*prescriber-identifying information is a mere commodity*" [204].

La teorizzazione non è però andata esente da critiche, suscitando le perplessità di chi ha visto nella figura del fiduciario informativo uno strumento di subdola elusione di

[201] Tale nozione, inizialmente sviluppata nel proprio blog personale in una riflessione dal titolo "*Information Fiduciaries in the Digital Age*" del 5 marzo 2014 (disponibile all'indirizzo *balkin.blogspot.com*), è stata poi più compiutamente riformulata in J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1183ss.

[202] Tale prospettiva può essere meglio compresa attraverso le parole di chi identifica il "*right to information privacy*" con un "*right to control your communication of personally identifiable information about me*" che finisce per tradursi nel "*right to have the government stop you from speaking about me*." E. VOLOKH, Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52, *Stan. L. Rev*., 2000, 1049, 1051.

[203] 131 S. Ct. 2653 (2011).

[204] Nelle parole della Corte: "*the creation and dissemination of information are speech within the meaning of the First Amendment*". *Sorrell v. IMS Health Inc*. 131 S. Ct. 2653 (2011), 2667. Cfr. J. GRIMMELMANN, The Law and Ethics of Experiments on Social Media Users, 13, *Colo. Tech. LJ*., 2015, 219, 255ss; J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1195; J. BAMBAUER, Is Data Speech?, 66, *Stan. L. Rev*., 2014, 57, 84ss; S.F. KREIMER, Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record, 159, *U. Pa. L. Rev*., 2011, 335ss.

ben più incisivi interventi legislativi[205]. Sul versante più squisitamente sostanziale, inoltre, l'assetto societario generalmente assunto dai titolari dei dati ha indotto alcuni a ravvisare una insanabile inconciliabilità tra i doveri di cura degli interessi degli utenti con i quali viene per tal via configurata una relazione fiduciaria e l'obbligo di non compromettere gli interessi economici dei propri azionisti e di tutti gli altri *stakeholders* coinvolti nello svolgimento del trattamento quale attività con scopo di lucro[206]. Infine, non è mancato chi ha visto in tale modello un mero "*restatement or refinement of consumer protection law, with particular application to online privacy"*[207], peraltro difficilmente implementabile[208] e suscettibile di promuovere una fuorviante rappresentazione dei giganti del mercato dei dati quali custodi prudenti e sensibili alle esigenze dei propri "clienti", favorendo un atteggiamento ancora più pericolosamente passivo degli interessati rispetto alla cura dei propri dati personali[209].

A dispetto di tali indubbie criticità, e sebbene la teorizzazione statunitense di un rapporto fiduciario sia stata necessitata da una lacuna legislativa in materia di trattamento dei dati personali assente nell'ordinamento eurounitario, la prospettiva può comunque giovare all'interprete domestico[210]. Ciò in quanto, teorizzando una terza via, diversa dalla

[205] Come efficacemente notato dagli Autori, infatti, "*a fiduciary approach might "nudge" companies like Facebook to "do the right thing," "without outright requiring it*"". Ancora, richiamando le parole di ZITTRAIN, allievo di BALKIN, si sottolinea come l'intento dichiarato della teorizzazione sia quello di proteggere i consumatori e correggere un evidente fallimento di mercato "*without the need for a heavy-handed government intervention*". L.M. KHAN, D.E. POZEN, A Skeptical View of Information Fiduciaries, 133, *Harvard. L. Rev*., 2019, 497, 503 e 537. Cfr. J. ZITTRAIN, How to Exercise the Power You Didn't Ask For, *Harv. Bus. Rev*., 2018. Sulla tradizionale propensione dell'ordinamento statunitense a rimettere la disciplina del regime di trattamento e circolazione dei dati personali a forme di autoregolamentazione di mercato si veda la breve ricognizione storica condotta in apertura al Capitolo III, *sub infra* §§3.1.-3.4.

[206] L.M. KHAN, D.E. POZEN, A Skeptical View of Information Fiduciaries, cit., 508-513.

[207] Ivi, 522. In senso analogamente critic v. J. GRIMMELMANN, When All You Have Is a Fiduciary, Law & Pol. Econ., 2019 disponibile all'indirizzo *www.lpeblog.org*.

[208] L.M. KHAN, D.E. POZEN, A Skeptical View of Information Fiduciaries, cit., 524. Cfr. *S. Davis*, The False Promise of Fiduciary Government, 89, *Notre Dame L. Rev*., 2014, 1145ss; E.J. LEIB, D.L. PONET, M. SEROTA, A Fiduciary Theory of Judging, 101, *Calif. L. Rev*., 2013, 699ss.

[209] L.M. KHAN, D.E. POZEN, A Skeptical View of Information Fiduciaries, cit., 540-541. Cfr. J.E. COHEN, The Regulatory State in the Information Age, 17, *Theoretical Inquiries L*., 2016, 369ss; A.M. FROOMKIN, Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements, *U. Ill. L. Rev.*, 2015, 1713ss; D.D. HIRSCH, Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, 41, *Ga. L. Rev*., 2006, 1ss; I. SAMUEL, The New Writs of Assistance, 86, *Fordham L. Rev*., 2018, 2873ss.

[210] L'affinità sostanziale dei doveri di cura teorizzati da BALKIN con gli obblighi del titolare disciplinati dal GDPR è ulteriormente confermata dal testo della proposta del *Data Care Act of 2019* (S.2961, 116th Congress 2019-2020) in cui è confluita buona parte della prospettiva fiduciaria descritta. In particolare, sebbene l'atto sia ancora in fase di consultazione, l'influenza delle teorizzazioni di BALKIN è principalmente confluita nella previsione di generali doveri di "cura, lealtà e confidenzialità", dove per "*duty of care*" si intende l'obbligo dell'Internet Service Provider (ISP) di *"(A) reasonably secure individual identifying data from unauthorized access; and (B) […] promptly inform an end user of any breach of the duty described in subparagraph (A) of this paragraph with respect to sensitive data of that end user*". La

proprietà e dal contratto, Balkin consente di conciliare la protezione dei dati personali (*data privacy*) e il principio di libera circolazione delle informazioni (ivi inteso come declinazione del *free speech*[211]*)* assumendo una prospettiva interindividuale in virtù della quale non è il contenuto del dato personale (*rectius* il suo legame con la personalità dell'interessato), ma il contesto relazionale dal quale trae origine, a fungere da *discrimen* tra informazioni "private" (*rectius* sensibili e personali al punto da risultare insuscettibili di formare oggetto di scambio) e informazioni che, al contrario, mostrano una valenza pubblica (*rectius* un potenziale economico strumentale al rafforzamento del mercato digitale) tale da rendere incostituzionali (*rectius* sbilanciati verso un ingiustificato *favor* per la posizione dell'interessato) eventuali limiti legislativi alla loro raccolta e diffusione[212]. In altri termini, il regime giuridico del dato personale verrebbe a trovare la sua ragione giustificatrice nella peculiarità della "relazione sociale" da cui originano[213].

Si passa quindi dalla funzione sociale dal dato come merce di scambio, alla relazione sociale instaurata tra utenti e prestatori di servizi online che, seppure non identica a quella intercorrente tra clienti e avvocati, medici o altre categorie professionali sottoposte a canonici obblighi deontologici di riservatezza, genera comunque la nascita

---

norma prosegue poi definendo il "*duty of loyalty*" come l'obbligo dell'ISP di non utilizzare le informazioni personali dei propri utenti (o altre informazioni inferite da tali dati) in modo tale da trarne vantaggio a detrimento del soggetto interessato, in particolare cagionando un "*reasonably foreseeable and material physical or financial harm to an end user*" ovvero in modo tale da risultare "*unexpected and highly offensive to a reasonable end user*". Infine, il "*duty of confidentiality*" è definito come il divieto di condividere o vendere dati personali in modo incompatibile con i doveri di cura e lealtà e, se del caso, limitare la vendita a soggetti che si siano contrattualmente obbligati verso il titolare cedente o alienante al rispetto degli stessi doveri di cura, lealtà e confidenzialità a cui quest'ultimo è soggetto. DATA CARE ACT OF 2019, Sec. (1), (2), e (3). Per più generiche riflessioni dottrinali su tali doveri di cura v. J.M. BALKIN, The First Amendment in the Second Gilded Age, 66, *Buff. L. Rev*., 2018, 979ss; A. DOBKIN, Information Fiduciaries in Practice: Data Privacy and User Expectations, 33, *Berkeley Tech. L.J.*, 2018, 1ss; T. Rostow, What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers, 34, *Yale J. On Reg*., 2017, 667ss.

[211] La dottrina statunitense, infatti, nel riflettere sul bene giuridico tutelato dal primo emendamento, tende ad individuarlo nel "*right to participate in the forms of meaning-making that shape who they are and that also help constitute them as individuals, whether or not their speech has much of a connection to politics*. […] *The First Amendment, in other words, protects cultural democracy as well as political democracy. Indeed, political democracy is made possible by the institutions of cultural democracy*." J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1211-1212 e Id., Cultural Democracy and the First Amendment, 110, *Nw. U. L. Rev*., 2016, 1053ss.

[212] Nelle parole dell'Autore: "[*i*]*nformation about clients that is obtained in the course of fiduciary relationships is not public discourse. Therefore, when a fiduciary communicates private information about a client to the public, the communication does not receive standard First Amendment protection, unless the dependent person - the client - permits the information to enter public discourse*." Così J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1219-1220.

[213] Nelle parole dell'Autore: "[*w*]*hat the contractual model gets right is that what makes privacy obligations enforceable notwithstanding the First Amendment is not the content of the speech but a legally enforceable social relationship; namely, contract. But other kinds of legally enforceable social relationships - namely, fiduciary relationships - may have the same effect*." Così Ivi, 1205, spec. nt. 104.

di una serie di affini obblighi di cura in capo ai titolari del trattamento nella misura in cui "*we trust them with sensitive information*"[214].

Tale considerazione è suffragata, secondo l'Autore, da un molteplice ordine di ragioni quali: (i) l'asimmetria informativa e di potere contrattuale che caratterizza la relazione da ISPs e utenti; (ii) la dipendenza che l'era digitale ha creato verso gran parte dei servizi offerti in rete a cui gli utenti spesso si trovano nella condizione di non poter (o voler) rinunciare; (iii) il carattere sostanzialmente infungibile di molti servizi offerti, le cui economie di scala rendono molto complessa la concorrenza e l'entrata in gioco di nuovi operatori; (iv) la consapevole arrendevolezza con cui gli utenti, rifugiandosi nelle vaghe ma rassicuranti dichiarazioni di *policy* dei titolari, accettano i rischi insiti nell'opaca complessità della modalità di raccolta e trattamento dei propri dati[215].

In conclusione, ai fini dell'analisi qui condotta, specialmente con riguardo alla disciplina dei processi decisionali automatizzati oggetto dei prossimi capitoli, la teoria dei fiduciari informativi mette bene in luce il principale limite dell'attuale dibattito dottrinale sul tema della natura giuridica dei dati personali e del loro regime di circolazione: l'esclusivo riguardo riservato alla dimensione individuale (e personale) del dato. In altri termini, oltre a mitigare alcune delle menzionate ambiguità interpretative sorte con riguardo al modello giuridico da applicare al rapporto obbligatorio tra titolare e interessato[216], la teorizzazione di peculiari doveri di cura in capo ai titolari del trattamento è, allo stesso tempo, utile a fornire una cornice assiologica, prima ancora che normativa,

[214] Ivi, 1221. In modo sostanzialmente analogo si è espresso N. RICHARDS, *Intellectual Privacy: Rethinking Civil Liberties In The Digital Age*, Oxford, Oxford University Press, 2015, 169ss. Cfr. J. Kang, Self-Surveillance Privacy, 97, *Iowa L. Rev*., 2012, 809ss; J. LITMAN, Information Privacy/Information Property, 52, *Stan. L. Rev*., 2000, 1283ss; N.M. RICHARDS, W. HARTZOG, Taking Trust Seriously in Privacy Law, 19, *Stan. Tech. L. Rev*., 2016, 431ss; N.M. RICHARDS, D.J. SOLOVE, Privacy's Other Path: Recovering the Law of Confidentiality, 96, *Geo. LJ*., 2007, 123ss.

[215] Nelle parole dell'Autore "*people and business entities act as information fiduciaries: (1) when these people or entities hold themselves out to the public as privacy-respecting organizations in order to gain the trust of those who use them; (2) when these people or entities give individuals reason to believe that they will not disclose or misuse their personal information; and (3) when the affected individuals reasonably believe that these people or entities will not disclose or misuse their personal information based on existing social norms of reasonable behavior, existing patterns of practice, or other objective factors that reasonably justify their trust*." J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1224-1225.

[216] Un esempio sono le conseguenze anacronistiche prodotte dalla *third party doctrine* che, analizzata *infra sub* Cap. III §*3.4.2*, tende a neutralizzare la presunzione di ragionevolezza dell'aspettativa di privacy avanzata dagli utenti rispetto ai dati personali spontaneamente condivisi con *Internet Service Providers*. Cfr. K. BRENNAN-MARQUEZ, Fourth Amendment Fiduciaries, 84, *Fordham L. Rev*., 2015, 611ss.

a tutte le relazioni che i titolari vengono ad intrattenere con gli interessati al di fuori della cornice, perlomeno latamente negoziale, del consenso.

Come si vedrà meglio nel prossimo capitolo, infatti, per effetto del passaggio dalla c.d. *Internet Society* alla c.d. "*Algorihmic Society*", i titolari del trattamento si avvalgono sempre più spesso di strumenti di analisi automatizzata dei dati raccolti per prendere decisioni (di business ma non solo) fortemente invasive della sfera giuridica di destinatari con i quali non intrattenevano necessariamente una pregressa relazione informativo-fiduciaria. Ciò avviene, ad esempio, in caso di decisioni individuali assunte sulla base sì di dati personali, ma inseriti in un procedimento automatizzato "allenato" da una vasta gamma di dati anonimizzati e fondato su modelli decisionali plasmati dai profili (di gruppo) per tal via inferiti.

In altri termini, configurare il ruolo che il titolare assume rispetto alla generalità dei consociati in termini affini a quelli di un "fiduciario informativo" consente di colmare il vuoto normativo lasciato dal GDPR rispetto al trattamento di dati sempre più frequentemente anonimizzati e, in tal modo, offrire una base ermeneutica da cui partire per affrontare quello che Balkin ha definito "[*t*]*he more interesting problem aris[ing] when algorithms use data about other people (or about large populations) in order to make predictions about users, and users have no relationship of trust or confidence with the enterprise that uses the algorithm*[217]."

1.7. Conclusioni preliminari

Alla luce di quanto sin qui esposto, si può preliminarmente concludere che, nell'ottica dell'analisi che seguirà, dal momento in cui viene ad essere integrata una delle basi giuridiche per il trattamento legittimo dei dati personali, questi ultimi intraprendono un processo di reificazione che progressivamente li allontana dalla sfera giuridica del soggetto interessato per attrarli sempre più in quella del titolare del trattamento.

In particolare, al momento della raccolta e in virtù di ciascuna delle condizioni di liceità del trattamento *ex* artt. 6 e 9 GDPR, il singolo dato personale diviene oggettivazione della personalità del soggetto interessato, inteso come istantanea rappresentazione di un

[217] J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1232.

frammento della sua identità temporalmente circoscritto e altro rispetto all'interessato, ma pur sempre riconducibile alla sua sfera giuridica. Rispetto a tale entità immateriale reificata, si formano due situazioni giuridiche soggettive, una riferibile al soggetto interessato e una riferibile al titolare del trattamento. Il primo acquisirà, infatti, dal momento della raccolta a quello della cancellazione del singolo frammento informativo, il diritto alla protezione dello stesso, ovvero al controllo della sua circolazione e manipolazione da parte del titolare del trattamento. Quest'ultimo, a sua volta, per effetto dell'integrazione di una delle basi giuridiche di cui agli artt. 6 e 9 GDPR, verrà a vantare un diritto soggettivo di libertà economica di natura fondamentale sul medesimo dato avente ad oggetto il suo sfruttamento economico.

In questa prospettiva, quindi, le basi giuridiche di cui agli artt. 6 e 9 GDPR, assurgono ad altri fatti idonei a produrre, ex art. 1173 cc, l'obbligazione del titolare del trattamento che, nel senso descritto nel precedente paragrafo, delinea un rapporto negoziale di stampo fiduciario col soggetto interessato, connotato da un peculiare dovere di cura dei diritti degli interessati nello sfruttamento economico dei propri dati personali. Tale dovere di cura è ben espresso in quell'obbligo di agevolare l'esercizio dei diritti dell'interessato che l'art. 12 GDPR espressamente configura rispetto alle tutele disciplinare negli artt. 15-22 GDPR.

Tale dovere di cura, legato al connotato personalistico che il dato personale presenta al momento della sua raccolta, viene progressivamente ad attenuarsi per effetto delle successive fasi di elaborazione del singolo frammento informativo. Di qui, la rilevanza delle riflessioni condotte in questo capitolo ai fini dell'analisi che seguirà sul diritto ad una spiegazione significativa delle decisioni automatizzate e del suo contenuto. A seguito dei processi di elaborazione (più o meno automatizzata) del complesso dei dati personali raccolti, infatti, questi vengono a perdere quella naturale riferibilità al soggetto da cui promanano, per divenire sempre di più sintetica rappresentazione di inferenze artificialmente estrapolate circa la sua personalità. Queste ultime, riconducibili alla generica nozione di profili o metadati, escono dalla sfera giuridica del soggetto interessato in quanto allo stesso solo indirettamente e statisticamente riferibili, ma, nell'ottica assunta nel presente capitolo, continuano pur sempre a formare oggetto di quella relazione negoziale di stampo fiduciario tra soggetto interessato e titolare. Ne consegue che, sebbene prodotto dell'esclusiva attività di analisi ed elaborazione del titolare del

trattamento, i metadati potranno sì formare oggetto di diritti di proprietà intellettuale (o meglio di quasi proprietà, i.e. segreto commerciale) del titolare del trattamento, ma continueranno a formare anche oggetto della relazione negoziale di stampo fiduciario tra titolare e interessato, giustificando così il diritto di quest'ultimo ad avervi accesso ove tali profili abbiano costituito il presupposto informativo di decisioni automatizzate ai sensi dell'articolo 22 GDPR. Se si assume una siffatta prospettiva relazionale, infatti, il maggior grado di reificazione del *profilo* rispetto al dato personale, pur avvicinandolo alla sfera dei diritti dominicali del titolare del trattamento, non fa perdere quel carattere personalistico della relazione instaurata col soggetto interessato da cui promanano i doveri di cura di cui il titolare rimane gravato e che giustificano, come si vedrà meglio nel prossimo capitolo, il diritto ad accedervi del destinatario di una decisione unicamente automatizzata prodotta sulla base degli stessi.

L'aver inquadrato la posizione giuridica del titolare del trattamento in un'ottica fiduciaria, ponendo quindi l'accento sul dovere di cura che lo stesso assume dal momento della raccolta del dato personale verso l'interessato, non implica ricondurre in capo al titolare diritti o doveri diversi da quelli disciplinati dal GDPR ma, al contrario, esportare quello stesso dovere di cura al di fuori del perimetro applicativo del Regolamento. In altri termini, attribuire stampo fiduciario alla relazione che si instaura tra titolare e interessato al momento del verificarsi di una delle basi giuridiche di cui agli artt. 6 e 9 GDPR significa spostare l'oggetto del dovere di cura dal dato personale in sé considerato al rapporto per tal via instaurato col soggetto a cui tale informazione è riferibile. Rapporto, quest'ultimo, che non si esaurisce nel momento in cui le attività di processazione del dato lo portano ad uscire dalla sfera di stretta riferibilità all'interessato per entrare in quella di privativa industriale del titolare nella sua nuova forma di metadato. È solo in quest'ottica, infatti, che si può giustificare un diritto di accesso al profilo (principale metadato inferito dai singoli dati personali) anche ove riferibile al gruppo e non al singolo interessato e perciò potenzialmente al di fuori del campo di applicazione del GDPR.

Ciò è particolarmente rilevante ai fini della disciplina del diritto ad una spiegazione dei processi decisionali automatizzati, in quanto, come si vedrà meglio nel prossimo capitolo, sono proprio i profili la matrice informativa più adatta a raggiungere la soglia di significatività delle informazioni rese al soggetto interessato ex artt. 15 e 22 GDPR.

Per questo motivo, al fine di meglio inquadrare la natura e i limiti del diritto di accesso agli stessi era imprescindibile condurre preliminarmente un'analisi della posizione giuridica che il titolare del trattamento viene ad assumere dapprima sul dato personale singolarmente considerato al momento del trattamento e poi all'esito del processo di elaborazione dello stesso, specialmente se utilizzato come base informativa per prendere decisioni automatizzate ex art. 22 GDPR.

Chiarito così il processo di reificazione che porta allo scollamento del profilo dalla sfera giuridica del soggetto interessato e al centro della posizione giuridica del titolare ma anche della relazione fiduciaria col soggetto interessato, è ora possibile proseguire la riflessione con l'analisi della struttura, del contenuto e dei limiti operativi e giuridici del diritto ad una spiegazione dei processi decisionali automatizzati che incidono significativamente sulla sfera giuridica dei soggetti interessati.

CAPITOLO SECONDO

IL DIRITTO ALLA COMPRENSIBILITÀ DEI PROCESSI DECISIONALI AUTOMATIZZATI

2.1. L'Articolo 22 GDPR

Il 25 maggio 2018 è entrato in vigore il GDPR il quale, fra tutte le novità introdotte, nella Sezione 4 del Capo III annovera fra i diritti dell'interessato una versione aggiornata della disposizione concernente i processi decisionali automatizzati relativi alle persone fisiche. L'articolo 22 GDPR, infatti, ripropone, con qualche puntualizzazione linguistica soltanto apparentemente formale, il "diritto [dell'interessato] di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato."

2.1.1. I prodromi normativi

La prima traccia normativa del principio ivi espresso è rinvenibile nell'ordinamento francese. In particolare, l'originario articolo 2 della Legge 78-17 del 6 gennaio 1978 *relative à l'informatique, aux fichiers et aux libertés* stabiliva che "*[a]ucune décision de justice impliquant une appréciation sur en comportement humain ne peut avoir pour fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé*" [218].

[218] A seguito dei vari interventi legislativi che hanno interessato la disposizione, la norma è oggi contenuta nell'articolo 47 della *Loi* 78-17 come da ultimo modificata dall'articolo 1 dell'*Ordonnance* n. 2018-1125 del 12 dicembre 2018 (in vigore dal 1 gennaio 2019), e stabilisce che "*Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception:*

1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du 27 avril 2016, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en oeuvre soient communiquées, à

Una norma analoga confluì poi nell'articolo 15 della previgente Direttiva 95/46/CE, rubricato "decisioni individuali automatizzate", in virtù del quale gli Stati membri riconobbero, per la prima volta in modo armonizzato a livello europeo, il diritto di ogni persona "di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc."[219].

Come acutamente affermato, sebbene la norma presenti indubbi tratti di peculiarità rispetto alle altre disposizioni in materia di protezione dei dati personali, e nonostante il carattere indiscutibilmente lungimirante della fattispecie disciplinata, la disposizione ha avuto un ruolo sorprendentemente sommesso nel corso degli oltre vent'anni di vita della Direttiva madre: la sua interpretazione o corretta applicazione non è stata mai sottoposta all'attenzione della Corte di Giustizia dell'Unione Europea (CGUE), né delle corti nazionali (salvo un unico noto caso affrontato della Corte federale della Germania)[220], né la dottrina si è interrogata in merito[221]. Per questo motivo, si parla di questa norma come di un "*second-class data protection right*"[222].

La disposizione, peraltro, non venne neppure inclusa nei cc.dd. *International Safe Harbor Privacy Principles* elaborati fra il 1998 e il 2000, e poi confluiti in quel *Safe Harbour Agreement* tra Unione Europea e Stati Uniti d'America, notoriamente invalidato dalla CGUE nel 2015 a fronte del ricorso dell'attivista Maximillian Schrems. Né

---

l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande;

2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 6 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en oeuvre à son égard. Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel."

[219] Articolo 15, comma 1 Direttiva 95/46/CE del Parlamento Europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U.C.E. L. 218/31.

[220] Sul punto di veda *infra* nel paragrafo terzo del presente capitolo.

[221] I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 77 e 80.

[222] Ivi, 78.

tantomeno ebbe maggiore fortuna l'anno successivo, essendo stata nuovamente trascurata dalla Commissione Europea e dal Governo statunitense nel corso delle negoziazioni che hanno portato al pur invalidato *EU-US Privacy Shield*[223].

Lo sviluppo dell'ecosistema *Big Data*, tuttavia, accompagnato dai rapidi avanzamenti delle applicazioni di Intelligenza Artificiale (IA), ha contribuito a innalzare il livello di attenzione su quella che oggi viene comunemente definita come "la vigilanza degli algoritmi"[224]. Espressione, questa, con la quale si intende riferirsi al controllo sugli effetti negativi e, più in generale, sulle conseguenze che i sistemi di IA sono potenzialmente in grado di produrre sulla sfera giuridica dei soggetti interessati[225]. La stessa Dichiarazione sull'Etica e la Protezione dei Dati Personali nei sistemi di Intelligenza Artificiale, adottata nell'ottobre 2018 nell'ambito nella 40esima Conferenza Internazionale dei Commissari per la Protezione dei Dati e la Privacy, al secondo principio promuove l'implementazione di una vigilanza continua sulle ripercussioni dell'intelligenza artificiale, assicurando, in particolare: (a) *l'accountability* di tutti i soggetti coinvolti[226]; (b) lo sviluppo di *best practices* per favorire una responsabilità collettiva e condivisa; (c) investimenti in campagne educative volte a innalzare il livello

[223] Vedi meglio *infra sub* Cap. III, §3.1. Per più esaustive riflessioni sul caso cfr. M.D. SCOTT, *Scott on Multimedia Law*, IV ed., Wolters Kluwer, New York, 2019, 93 ss; S. SICA, V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei* Safe Harbour Privacy Principles, in. V. ZENO ZENCOVICH e G. RESTA (a cura di), *La protezione transnazionale dei dati personali: dai* Safe Harbour Principles *al "*Privacy Shield*"*, Roma Tre E-Press, Roma, 2016, 137 ss; K.J. FIETKIEWICZ, M. HENKEL, *Privacy Protecting Fitness Trackers: An Oxymoron or Soon to be Reality?*, in G. MEISELWITZ (a cura di), *Social Computing and Social Media. User Experience and Behavior*, Vol. I, Springer International Publishing, Cham, 2018, 438ss; R. PANETTA, *Il trasferimento all'estero dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019, 364 ss.

[224] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Privacy e intelligenza artificiale: vigilare sugli algoritmi. Il contributo del Garante italiano nel Comitato consultivo della Convenzione 108*, Notiziario n. 451 del 25 marzo 2019, disponibile in <www.garanteprivacy.it>. Sul punto, si vedano anche le osservazioni di ALESSANDRO MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasburgo, 25 gennaio 2019 (T-PD(2018)09Rev), 17ss.

[225] COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, (Starsburgo, 25 gennaio 2019, T-Pd(2019)01), 3.

[226] Cfr. E. LUCCHINI GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 82 ss, nonché D. POLETTI, M.C. CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 377 ss.

di consapevolezza dei rischi da parte della società; e (d) lo sviluppo di processi di *governance* trasparenti, ideati col supporto di comitati etici *ad hoc*[227].

2.1.2. Il contesto tecnologico: *Big Data* e *Deep Learning*

Il Consiglio d'Europa definisce oggi l'Intelligenza Artificiale (IA) come quel complesso di scienze, teorie e tecniche finalizzate a riprodurre le abilità cognitive di un essere umano per mezzo di una macchina, al fine ultimo di affidargli compiti finora delegati ad operatori umani[228]. Eppure, a dispetto di ciò che la tempistica del fermento legislativo potrebbe far presumere, il complesso funzionamento delle reti neurali umane iniziò a suscitare un interesse multidisciplinare sin dagli anni '40 del secolo scorso, approdando alla prima pietra miliare nel 1950, con la presentazione del test sviluppato da Alan Turing per dimostrare la capacità di una macchina di imitare i processi mentali al punto da ingannare un interlocutore umano circa la sua artificialità (c.d. "*imitation game*")[229]. Risale poi al *workshop* organizzato presso il Dartmouth College del 1956, l'attribuzione della paternità dell'espressione "Intelligenza Artificiale". Successivamente, la ricerca sull'IA ha vissuto fasi di forte scetticismo e abbandono,

[227] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Declaration on Ethics and Data Protection in Artifical Intelligence* (40th International Conference of Data Protection and Privacy Commissioners, Bruxelles, 23 ottobre 2018), 4, § 2. Cfr. F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della* blockchain, *intelligenza artificiale e IoT*, Ipsoa, Milano, 2018, 193 ss.

[228] PORTALE DEL CONSIGLIO D'EUROPA, Glossario, Intelligenza Artificiale (voce), disponibile all'indirizzo <*www.coe.int/en/web/artificial-intelligence/glossary*>. Dal canto suo la recente proposta euronitaria di un regime di responsabilità civile per l'intelligenza artificiale definisce i sistemi di IA come "un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici". Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), Art. 3(1)(a).

[229] A.M. TURING, Computing Machinery and Intelligence, 49, *Mind*, 1950, 433ss. La tesi venne poi confutata a livello filosofico dal celebre esperimento mentale della c.d. "*Chinese room*", teorizzato da John Searle negli anni '80 e che può essere così brevemente ripercorso: immagina di essere chiuso in una stanza. Nella stanza si trova una cesta piena di simboli cinesi e, sebbene tu non conosca una parola di cinese, ti viene fornito un manuale di istruzioni (scritto nella tua lingua), grazie al quale riesci ad assemblare le sequenze di simboli da trasmettere all'esterno della stanza. Poniamo il caso che coloro che sono fuori dalla stanza stanno effettuando un qualche versione del test di Turing, e che tu diventi così bravo a seguire le istruzioni del manuale che riesci a comunicare con l'esterno della stanza con frasi cinesi talmente avanzate da convincere coloro che stanno eseguendo il test che tu sia madrelingua cinese. Hai passato il test di Turing, ma continui a non capire una parola di cinese. Sulle implicazioni giuridiche della mancanza di quella che Searle ha definito come intenzionalità, rispetto ai potenziali rischi posti dai sistemi di c.d. *strong artificial intelligence* (o strong AI) si veda *infra* nel paragrafo. J.R. SEARLE, Minds, Brains and Science, 3, *Behavioral and Brain Sciences*, 1980, 3, 417 ss. Cfr. L.B. SOLUM, Legal Personhood for Artificial Intelligences, 70, *North Carolina Law Review*, 4, 1992, 1231ss.

alternate a epoche, come quella attuale, di grande ottimismo e attenzione[230]. Tuttavia, fu soltanto a partire dai primi anni '90 dello scorso secolo che la curva del successo dell'IA registrò l'impennata responsabile dell'attenzione legislativa autrice della disposizione oggetto di analisi di questo capitolo.

Tale svolta non è imputabile ad una particolare evoluzione dei sistemi di IA (già all'epoca altamente performanti), quanto piuttosto allo sviluppo dell'ecosistema tecnologico in cui questa si è venuta a collocare. In particolare, un ruolo decisivo è stato svolto dalla crescita del potere computazionale e, soprattutto, dalla disponibilità e capacità di gestire Volumi di dati, prodotti ad una Velocità senza precedenti, perciò aggiornati in tempo reale (Varietà) e quindi sempre più accurati e dettagliati (Veridicità). Sono queste, infatti, le cc.dd. quattro "V" che caratterizzato i *Big Data*[231].

Il cambiamento che ha reso possibile il pieno sfruttamento delle potenzialità *in nuce* già insite negli esistenti sistemi di IA, quindi, è rinvenibile nella opportunità, aperta a questi ultimi dai *Big Data*, di analizzare una mole senza precedenti di dati attinenti ad ogni aspetto del reale, individuando correlazioni tra gli stessi, fonti di nuova conoscenza (si parla, infatti, di *Knowledge Discovery in Databases*)[232]. In particolare, siffatto flusso di informazioni è principalmente imputabile alla costante creazione di cc.dd. *User-generated Contents* (quali, ad esempio, le interazioni nei *social networks* o le parole

[230] G.F. ITALIANO, Intelligenza Artificiale: passato, presente, futuro in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018, 209ss.

[231] Cfr. M. N. HELVESTON, Consumer Protection in the Age of *Big Data*, 93, *Wash. U. L. Rev*., 2016, 859, 867; F. MATTASSOGLIO, *Big Data*, in M. T. PARACAMPO (a cura di), *FinTech: Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli Editore, Torino, 2017, 69ss; T. MAURO, *I Big Data tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 651 ss; V. MAYER-SCHONBERGER e T. RAMGE, *Reinventing Capitalism in the Age of Big Data*, John Murray Publishers, Londra, 2018; M. HILDEBRANDT, *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Northampton, 31 ss.

[232] Il *data mining* è definito come il "*nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data*." In particolare, l'inizio di questo processo viene tradizionalmente ascritto alla selezione dei dati, seguito poi dalla rimozione delle interferenze suscettibili di minare l'accuratezza del risultato dell'analisi. I dati, così depurati, vengono poi trasformati in una forma più facilmente elaborabile dal sistema informatico, conseguentemente trattati per rilevare correlazioni tra gli stessi, oggetto, infine, di una valutazione complessiva volta a mettere in luce le nuove informazioni (i.e. *knowledge*) estrapolate dai dati iniziali attraverso questo procedimento. U. FAYYAD, G. PIATETSKY-SHAPIRO e P. SMYTH, From Data Mining to Knowledge Discovery in Databases, 17, *AI Magazine*, 3, 1996, 37, 39ss. Cfr. T. ZARSKY, *Transparency in Data Mining: From Theory to Practice*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*, Springer, Berlino, 2013, 307.

chiave inserite in motori di ricerca online)[233], così come alla digitalizzazione della pressoché totalità di dati strutturati (informazioni sanitarie, finanziarie, ecc.), nonché alla emergente mole di dati prodotti dalla comunicazione *machine-to-machine* (prima fra tutte quella ascrivibile ai dispositivi di *Internet of Things*)[234].

È in questo contesto che si è progressivamente affermata la tendenza ad utilizzare tecniche di *machine learning* (ML) a fini decisionali[235]. Il ML è una sottocategoria dell'intelligenza artificiale, utilizzata per estrarre descrittori dai dati. Più specificamente, potendo prescindere dall'intervento umano, si tratta di una tecnica c.d. passiva di analisi dei dati[236]. Tradizionalmente, inoltre, si distingue tra *machine learning* supervisionato e non supervisionato. In quest'ultimo, a differenza del primo, le categorie attraverso le quali classificare il flusso di dati non sono predefinite dal programmatore, ma vengono stabilite autonomamente dall'algoritmo stesso che non viene a tal fine preventivamente "addestrato"[237].

La declinazione di ML che maggiormente ha beneficiato dall'evoluzione dei *Big Data* è il c.d. *deep learning*, una sottocategoria del *machine learning* non supervisionato,

---

[233] GENEVA ASSOCIATION, *Big Data and Insurance: Implications for Innovation, Competition and Privacy*, Zurigo, 2018, 8. Cfr. E. GERMANI, L. FEROLA, Il *wearable computing* e gli orizzonti futuri della *privacy*, 1, *Diritto dell'informazione e dell'informatica*, 2014, 75 ss.

[234] In particolare, si tratta di "un'evoluzione della rete Internet grazie alla quale gli oggetti interagiscono tra loro attraverso sensori e senza l'intervento umano, scambiandosi informazioni e accedendo ai contenuti presenti nelle banche dati". In questo senso si è espressa M.C. GAETA, La protezione dei dati personali nell'*Internet of Things*: l'esempio dei veicoli autonomi, 1, *Diritto dell'informazione e dell'informatica*, 2018, 147 ss. Per l'analoga definizione del Gruppo di lavoro articolo 29 si veda GRUPPO DI LAVORO ARTICOLO 29, *Opinion 8/2014 on the on Recent Developments on the Internet of Things*, adottata il 16 settembre 2014 (WP 223), 4. Cfr. A. MANTELERO, G. VACIAGO, *Internet of Things (IoT)*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 569 ss; M. MACCARTHY, *In defence of Big Data Analytics*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018, 47 ss; F. FAINI, *Big Data e* Internet of Things*:* Data Protection *e* Data Governance *alla luce del regolamento europeo,* in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 259; E. TOSI, *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy*, in ID. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., 36 ss.

[235] A proposito del *machine learning*, si è detto che è "un algoritmo che impara dai dati e arriva a un *output* senza avere regole predefinite all'inizio del percorso." Queste le parole di ANDREINA MANDELLI, *Intelligenza artificiale e marketing: agenti invisibili, esperienza, valore e business*, Egea, Milano, 2018, §2.3.

[236] Per una riflessione di più ampio respiro sulle caratteristiche dell'intelligenza artificiale cfr. M. IASELLI, *Intelligenza artificiale e robotica*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 281 ss.

[237] Così si esprime Danilo Benedetti nel volume di G. D'ACQUISTO e M. NALDI, *Big Data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli Editore, Torino, 2017, 15-16.

denominato "profondo" perché caratterizzato dall'essere strutturato su più livelli di reti neurali artificiali, ognuno dei quali produttore di un *output* che opererà come *input* nel livello successivo[238]. Questa particolarità del *deep learning* è ciò che rende la sua capacità computazionale "scalabile", ossia suscettibile di migliorare le proprie prestazioni all'aumentare dei dati disponibili (di qui il suo particolare successo nel contesto *Big Data*)[239].

L'attitudine all'autoapprendimento della rete neurale dei sistemi di *deep learning*, quindi, colloca quest'ultimo in quella che John Searle ha definito come "*strong AI*", poiché non si limita ad essere uno strumento a supporto della mente umana, ma si propone come una "mente" autonoma, dotata di una propria capacità di comprensione e di un proprio *status* cognitivo[240].

Dal punto di vista più squisitamente empirico, questi sviluppi tecnologici si sono tradotti in processi decisionali automatizzati sempre più invasivi, applicati ad una pletora sempre più ampia di settori. L'esempio più paradigmatico è quello del noto Sistema del Credito Sociale cinese, avviato in alcune parti della Cina dal 2014 al fine di sfruttare le nuove opportunità tecnologiche di controllo sociale a supporto della c.d. "cultura della sincerità". Il sistema si declina come un programma di credito di massa, in virtù del quale le potenzialità dei *Big Data* vengono sfruttate per raccogliere e analizzare dati strutturati (e non) provenienti dai quarantacinque organismi partecipanti, inclusa la Corte popolare suprema. Tali informazioni sono poi trattate al fine di attribuire ad ogni cittadino un punteggio, in virtù del quale gli potrà essere riconosciuta (o negata) la concessione di alloggi popolari, l'acquisto di azioni o altre forme di accesso al sistema finanziario, la possibilità di effettuare acquisti di lusso, di arruolarsi, di ricevere titoli onorari e molto altro[241].

---

[238] Per le questioni giuridiche sollevate dalle varie applicazioni dell'Intelligenza Artificiale, e relativa ricognizione, si veda anche E. PALMERINI, Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea, 6, *Responsabilità civile e previdenza*, 6, 2016, 1815B ss.

[239] Cfr. N. BOLDRINI, *AI. Artificial Intelligence*, Milano Finanzia S.p.a., Milano, 2018; M. HODNETT e J.F. WILEY, *Deep Learning Essentials*, Packt Publishing, Birmingham, 2018, 9ss.

[240] J.R. SEARLE, Minds, Brains and Science, 3, *Behavioral and Brain Sciences*, 1980, 3, 417 ss. Utilizzando le affini categorizzazioni di Flanagan, invece, il *deep learning* sarebbe ascrivibile alla categoria della c.d. *Strong psychological AI*, in virtù della quale, invertendo la prospettiva, la stessa mente umana sarebbe un computer e quindi replicabile dai sistemi di intelligenza artificiale. O.J. FLANAGAN, *Science of the Mind*, 2 ed., MIT Press, Massachusetts, 1991, 242 ss.

[241] Le origini dell'iniziativa risalgono al 2006, quando la banca popolare cinese creò un'unica agenzia di valutazione del merito creditizio nota come il Centro di referenze per il credito. Da notare, che nel contesto cinese il termine "credito" richiama qualcosa di più della mera capacità di restituire un

Analogo è il funzionamento di sistemi privati di *credit scoring*, seppure di matrice più squisitamente finanziaria, come il *Sesame Credit* sviluppato dalla controllata di Alibaba[242], o il Fico *score* creato dalla Fair Isaac Corporation, una delle principali società di analisi dei dati statunitense e utilizzato dalla quasi totalità dei principali finanziatori[243]. Entrambi i sistemi richiamati, rappresentano due delle più note espressioni di quell'approccio alla valutazione del merito creditizio che, avvalendosi del contesto *Big Data*, segue la filosofia del c.d. "*all data is credit data*"[244].

Questa rapida panoramica delle potenziali applicazioni del binomio *Big Data*-Intelligenza Artificiale, per quanto necessariamente parziale, rende comunque più che adeguatamente la misura del valore economico progressivamente assunto dai dati personali[245]. In particolare, richiamando le parole di Alessandro Mantelero "[*t]here is an emerging tendency towards a technocratic and market-driven society, which pushes for personal data monetisation, forms of social control and "cheap & fast" decision-making solutions*"[246].

---

finanziamento, ma implica una dimensione più personalistica legata al più generico e onnicomprensivo aspetto dell'affidabilità sociale di un individuo. Già a quell'epoca, infatti, l'agenzia raccoglieva informazioni di natura non finanziaria provenienti, ad esempio, da aziende di telecomunicazioni. Dal 2016, poi, il programma è stato integrato dal c.d. *Joint Punishment System*, ispirato al principio della sanzione "sproporzionata", originariamente concepito per rafforzare l'ottemperanza di provvedimenti giurisdizionali e oggi esteso ai molteplici aspetti di vita quotidiana richiamati nel testo. Cfr. R. CREEMERS, *China's Social Credit System: An Evolving Practice of Control*, 9 maggio 2018. Disponibile all'indirizzo <ssrn.com/abstract=3175792>. Cfr. S. VIVIENNE e P. THORNTON, *Beyond Implicit Political Dichotomies and Linear Models of Change in China*, in ID. (a cura di), *To Govern China: Evolving Practices of Power*, Cambridge, Cambridge University Press, 2017, 4ss; China invents the digital totalitarian state. The worrying implications of its social-credit project (*The Economist*, Pechino, 17 dicembre 2016); C. NGUYEN, China might use data to create a score for each citizen based on how trustworthy they are (*Business Insider*, 26 ottobre 2016); A. XU, Chinese Judicial Justice on the Cloud: A Future Call or a Pandora's Box? An Analysis of the 'Intelligent Court System' of China, 26, *Information & Communications Technology Law*, 1, 59, 2017, 62ss.

[242] Cfr. C. UDEMANS, *Alipay's Sesame Credit now accepted by Canada for visa applications* (Technode, 23 novembre 2018); N. KOBIE, *The complicated truth about China's social credit system* (Wired, 21 gennaio 2019); L. YILUN CHEN, *Jack Ma's Ant Apologizes for Baiting Users Into Credit System* (Bloomerang, 4 gennaio 2018); A. VISWANATHA e K. O'KEEFFE, *Before It Was Hacked, Equifax Had a Different Fear: Chinese Spying* (The Wall Street Journal, 12 settembre 2018).

[243] MyFico, Credit Education, disponibile all'indirizzo <www.myfico.com/credit-education>.

[244] In questo senso, M. HURLEY e J. ADEBAYO, Credit Scoring in the Era of *Big Data*, 18 *Yale J.L. & Tech*., 2016, 148, 164ss. Cfr. S. AZIZ e M. DOWLING, Machine Learning and AI for Risk Management, in T. LYNN, J.G. MOONEY, P. ROSATI e M. CUMMINS (Eds), *Disrupting Finance: FinTech and Strategy in the 21st Century*, Palgrave Macmillian, Dublino, 2019, 35ss.

[245] Cfr. G. ALPA, *La "proprietà" dei dati personali*, cit., 11 ss; J. VAN DIJCK, Datafication, dataism and dataveillance: *Big Data* between scientific paradigm and ideology, 12, *Surveillance & Society*, 2, 197 ss; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 23 ss.

[246] ALESSANDRO MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 25 January

2.1.3. La *ratio* e la natura del diritto (*rectius* divieto)

L'emersione delle minacce tecnologiche fin qui brevemente descritte ha favorito la presa di coscienza, da parte del legislatore europeo, della rinnovata attualità della *ratio* sottesa alla disposizione fin dalla sua previgente formulazione[247]. Sebbene i lavori preparatori al GDPR non lascino trapelare riflessioni sul punto, infatti, si ritiene che l'esigenza perseguita dall'articolo 22 GDPR, sul solco dell'articolo 15 Dir. 95/46/CE, sia rimasta quella di contrastare l'indebolimento della capacità dei soggetti interessati di incidere attivamente sul contenuto delle decisioni che li riguardano[248].

Gli sviluppi tecnologici summenzionati, tuttavia, hanno reso questo proposito bidirezionale.

Nella prospettiva dei soggetti interessati, si pone l'esigenza di garantire la possibilità di sottrarsi a decisioni basate esclusivamente sul trattamento dei propri dati personali, salvaguardando l'esistenza di alternative[249].

A tal proposito, il Gruppo di lavoro articolo 29 ha sostenuto che l'articolo 22 GDPR, essendo formulato in termini negativi (come il "diritto a non essere"),

---

2019, T-PD(2018)09Rev), 5; S. SPIEKERMANN, *Ethical IT Innovation. A Value-Based System Design Approach*, Taylor & Francis Group, Boca Raton, 2016, 152-153.

[247] A tal proposito, basti pensare che in occasione del *World Economic Forum* svoltosi a Davos nel gennaio 2019, il CEO di Microsoft ha elogiato l'iniziativa presa dal legislatore europeo col GDPR, arrivando a qualificare il diritto alla privacy (*rectius* alla protezione dei dati personali) come un diritto umano, la cui tutela rappresenta una delle principali sfide poste dallo sviluppo dei sistemi di intelligenza artificiale. CERI PARKER, Privacy is a human right, we need a GDPR for the world: Microsoft CEO (*World Economic Forum*, 24 gennaio 2019) disponibile all'indirizzo <www.weforum.org/agenda/2019/01/privacy-is-a-human-right-we-need-a-gdpr-for-the-world-microsoft-ceo>.

[248] Già nel 2017, il Consiglio d'Europa, nel redigere le linee guida sui *Big Data*, sottolineava l'importanza di salvaguardare l'effettiva libertà degli agenti umani nel prendere decisioni. CONSULTATIVE COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108), *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data* (Consiglio d'Europa, 23 gennaio 2017) (T-PD(2017)01), §7. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 83 ss.

[249] Sul punto, il Comitato consultivo della Convenzione 108, nell'enfatizzare le potenzialità mostrate dall'Intelligenza Artificiale a fini decisionali, ha sottolineato la necessità di garantire un approccio "*human rights by-design*". Con questa espressione, il Comitato ha voluto quindi ribadire la necessità di implementare cautele volte a salvaguardare la centralità della dignità umana nello sviluppare processi decisionali automatizzati. COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, (Starsburgo, 25 gennaio 2019, T-Pd(2019)01), § 3.

sembrerebbe fissare un vero e proprio divieto di assumere decisioni interamente automatizzate. In altri termini, il Gruppo di lavoro articolo 29 ha ritenuto che, seppure possa essere individuato nell'articolo 22 co.1 GDPR un diritto attivo, questo non si qualificherebbe come diritto di opposizione, ma come una delle "garanzie che devono essere applicate nei casi in cui è consentito il processo decisionale automatizzato [articolo 22, paragrafo 2, lettere da a) a c)] – [al pari del] diritto di ottenere l'intervento umano, di esprimere la propria opinione e di contestare la decisione- […] poiché è vietato lo svolgimento del trattamento descritto nell'articolo 22, paragrafo 1, su altre basi"[250].

A supporto di questa interpretazione, si adducono un argomento letterale e uno sistematico. In virtù del primo, il Gruppo di lavoro articolo 29 ritiene che la collocazione dell'articolo 22 GDPR in una sezione denominata "Diritto di opposizione *e* processo decisionale automatizzato relativo alle persone fisiche"[251], sia indicativa dell'intenzione del legislatore europeo di fissare un diritto di opposizione nel solo articolo 21 GDPR[252]. Quest'ultimo, peraltro, al comma 4 disciplina un obbligo di informazione assente nel dettato dell'articolo 22 GDPR, a riprova della irrilevanza del coinvolgimento attivo dell'interessato ai fini dell'operatività della norma[253].

Dal punto di vista sistematico, invece, il Gruppo di lavoro articolo 29 sottolinea come, privilegiando l'interpretazione opposta, si priverebbe di senso la previsione per cui, nei casi di cui all'articolo 22, co.2, lett. (a) e (c), il soggetto interessato ha diritto ad ottenere l'intervento umano. Ciò nella misura in cui, esercitando il diritto di opposizione

[250] In particolare, il Gruppo di lavoro articolo 29 specifica che, mentre gli articoli 15-18 e 20-21 GDPR "riguardano l'interessato che esercita attivamente i suoi diritti", gli articoli 13 e 14 "riguardano i doveri che il titolare del trattamento deve adempiere senza alcun coinvolgimento attivo dell'interessato." Ne consegue, continua il Gruppo di lavoro, che "l'inclusione dell'articolo 22 in tale capo [i.e. il capo III dedicato ai diritti dell'interessato] non significa di per sé che si tratti di un diritto di opposizione." GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 39.

[251] Corsivo aggiunto.

[252] Circa il diritto di opposizione si veda, fra gli altri, il recente contributo di G. DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato"*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019, 251 ss.

[253] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 39. Cfr. M. BRKAN, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, 11, *International Journal of Law and Information Technology*, 2019, 1-31; T. ZARSKY, The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making, 41, *Science, Technology, & Human Values*, 2016, 118–32.

teorizzato rispetto al primo comma, renderebbe superfluo ogni ulteriore intervento umano[254].

In realtà, per quando apprezzabile nelle intenzioni, questa interpretazione è tutt'altro che univoca, poiché si espone a confutazioni su entrambi i fronti.

Sul versante testuale, la mancata previsione di un dovere informativo in capo al titolare del trattamento nell'articolo 22 GDPR, non è indicativa dell'inesistenza di un obbligo in tal senso. In particolare, come si vedrà meglio nei prossimi paragrafi, gli articoli 13 co.2 lett. b e 14 co.2 lett. g GDPR pongono in capo al titolare del trattamento il dovere di fornire all'interessato informazioni circa "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22 GDPR, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"[255].

Peraltro, al di là delle differenti soluzioni adottate dagli Stati membri in sede di recepimento della Direttiva madre[256], quando il legislatore europeo ha voluto vietare i processi decisionali automatizzati *tout court* lo ha fatto espressamente. Ad esempio, l'articolo 6 co.5 Direttiva 2016/681/UE sull'uso dei *Passenger Name Records* a fini di prevenzione e contrasto al terrorismo stabilisce che, nel caso in cui un individuo sia qualificato come potenziale criminale sulla base del trattamento automatizzato dei PNR,

[254] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 40. Cfr. F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, Torino, 2016, 266 ss; S. BONAVITA (a cura di), *Società delle tecnologie esponenziali e* General Data Protection Regulation. *Profili critici nella protezione dei dati*, Ledizioni LediPublishing, Milano, 2018; G. RESTA, *Dignità, persone e mercati*, Giappichelli Editore, Torino, 2014, 338 ss.

[255] Cfr. F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018, 178 ss; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario. Regolamento (UE) 2016/679 del 27 aprile 2016 - Decreto di adeguamento D.Lgs. n. 101/2018 - Codice privacy D.Lgs. n. 196/2003*, Ipsoa, Milano, 2018, 135 ss;

[256] Ad esempio, mentre il Belgio aveva optato per un vero e proprio divieto, la Norvegia si era limitata a conferire agli interessati la facoltà di opporsi a decisioni basate sul trattamento automatizzato dei propri dati personali. L'Italia, dal canto suo, aveva adottato un approccio misto, vietando decisioni automatizzate basate esclusivamente sul trattamento dei dati personali in ambito amministrativo e giudiziale, ammettendole, invece, nel settore privato, pur dando la possibilità agli interessati di opporsi. Cfr. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 86ss.

tale decisione debba essere sempre oggetto di una revisione su base individuale e con mezzi non automatizzati[257].

Lo stesso può dirsi con riferimento alla sostanziale riproduzione della norma nell'articolo 11 della Direttiva 2016/680/UE[258], in occasione della quale il legislatore europeo ha più esplicitamente statuito che "una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato *sia vietata salvo che sia autorizzata* dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento *e che* preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento"[259].

È pur vero, tuttavia, che l'analisi dei lavori preparatori del testo dell'articolo 22 GDPR sembrerebbero fornire argomenti a favore della tesi del divieto.

In primo luogo, si potrebbe sostenere che, ove il legislatore europeo avesse voluto introdurre un diritto di opposizione avrebbe recepito la più esplicita formulazione proposta dal Comitato per le libertà civili, la giustizia e gli affari interni, in persona del suo *Rapporteur* Jan Philipp Albrecht. In particolare, il considerando 58 proposto dal Comitato avrebbe dovuto specificare che "fatta salva la legittimità del trattamento dei dati, ogni persona fisica ha il diritto di opporsi alla profilazione. La profilazione che

[257] Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi G.U. L. 119/132. Anche l'*International Labour Office* (ILO), pur ispirandosi all'articolo 15 Dir. 95/46/CE, ha elaborato i principi per cui: (i) le decisioni concernenti un lavoratore non possono essere basate unicamente sul trattamento automatizzato dei suoi dati personali; (ii) i dati personali del lavoratore raccolti per mezzo di monitoraggio elettronico, non possono essere gli unici fattori presi in considerazione nella valutazione della sua performance. ILO, *Code of practice on the protection of workers' personal data*, Geneva, 1997.

[258] Articolo 11 Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, G.U. L.119/89. Tale norma, peraltro, sostanzialmente replica quanto statuito dall'articolo 7 della previgente decisione quadro 2008/977/GAI. Cfr. S. RICCI, *Il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1135 ss.

[259] Corsivo aggiunto. Al di fuori del contesto europeo, peraltro, disposizioni analoghe all'articolo 22 GDPR si ritrovano anche in alcuni Stati africani, come ad esempio la normative sulla protezione dei dati adottata nel 2008 dal Senegal, nel 2011 dall'Anagola, nel 2012 dal Leshoto e nel 2013 dal Sud Africa. Cfr. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 81, spec. nt. 17 e 19.

conduce all'adozione di misure che producono effetti giuridici in capo all'interessato o che, similarmente, producono significativi effetti nei suoi confronti deve essere ammessa solo se autorizzata dalla legge, condotta nel corso della conclusione o esecuzione di un contratto, o preceduta dal consenso esplicito dell'interessato. In ogni caso, tale trattamento dovrebbe essere soggetto ad adeguate salvaguardie, inclusi il dovere di fornire informazioni specifiche all'interessato e il diritto di ottenere una valutazione umana"[260].

Al di là del ristretto scopo di applicazione della norma, limitato alla sola profilazione[261], la formulazione in termini di diritto attivo proposta dal Comitato colmava entrambe le lacune denunciate dal Gruppo di lavoro articolo 29. Da un lato, infatti, la disposizione stabiliva a chiare lettere il diritto degli interessati di obiettare alla profilazione, richiamando le modalità fissate dalla norma sul diritto di opposizione[262]. Dall'altro, includeva la diretta menzione del diritto degli interessati ad essere informati sull'esistenza di siffatto diritto[263].

Ulteriore riprova del valore di divieto generale attribuito dal legislatore europeo al "diritto a non essere sottoposto" ad una decisione automatizzata, proviene anche dall'obiezione mossa dal Comitato per il mercato interno e la protezione dei consumatori, in persona del *Rapporteur* Lara Comi. Quest'ultima, infatti, pur supportando l'implementazione di un impianto normativo ispirato alla massima protezione dei dati personali senza porre nessun onere proattivo in capo agli interessati, criticava il carattere eccessivamente generico del divieto così come formulato dalla Commissione. A tal proposito, il Comitato proponeva di inserire una specificazione, fissando così il diritto degli interessati di non essere soggetti a decisioni "inique o discriminatorie" basate unicamente su un trattamento automatizzato "volto a valutare determinati aspetti relativi

[260] RAPPORTEUR JAN PHILIPP ALBRECHT, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Civil Liberties, Justice and Home Affairs, 21 novembre 2013), 25.

[261] Sull'ampliamento dello scopo di applicazione dell'articolo 22 GDPR e sulla differenza tra trattamento automatizzato e profilazione si veda meglio *infra* §2.2.1.

[262] Cfr. I. DESTRI e A.M. LOTTO, *La profilazione*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 134 ss.

[263] RAPPORTEUR JAN PHILIPP ALBRECHT, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Civil Liberties, Justice and Home Affairs, 21 novembre 2013), 93.

allo stesso." In questo modo, focalizzando l'attenzione sui soli impieghi negativi delle tecniche di profilazione, il Comitato riteneva sarebbe stato possibile adottare un atteggiamento legislativo tecnologicamente neutro e raggiungere un miglior bilanciamento tra le esigenze dei consumatori e quelle del mercato [264].

Tornando alla prospettiva sistematica, invece, si potrebbe obiettare al Gruppo di lavoro articolo 29 che, per i casi in cui l'articolo 22 co.2 GDPR esclude la possibilità dell'interessato di sottrarsi alla decisione unicamente automatizzata, il legislatore ha previsto dei contrappesi, fra cui è annoverabile il diritto di ottenere l'intervento "*da parte del titolare del trattamento*"[265]. È evidente, quindi, che l'opposizione eventualmente esercitata dal soggetto interessato *ex* articolo 22 co.1 GDPR non sia riconducibile all'intervento umano di cui all'articolo 22 co.3 GDPR. Innanzitutto, perché quest'ultima disposizione riguarda le ipotesi in cui siffatto diritto venga a mancare e, in secondo luogo, perché è la norma stessa a specificare che l'intervento umano in questione riguarda il lato del decisore, ed è quindi volto a garantire una (ri)valutazione umana della determinazione automatizzata[266].

Di qui la nuova (seconda) direzione del timore sotteso alla *ratio* della norma, introdotta dalle nuove potenzialità tecnologiche: l'eccessivo affidamento, da parte dei decisori umani, nella validità e correttezza della decisione presa dalla macchina (c.d. *overreliance*)[267]. Seppure apparentemente oggettivo ed incontrovertibile, infatti, il

[264] RAPPORTEUR LARA COMI, *Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 28 gennaio 2013, 420ss.

[265] Corsivo aggiunto.

[266] Come messo in luce da Mantelero, infatti, il c.d. *machine-generated bias* è diverso dallo *human bias* e per questo è necessario evitare "*the allure of mathematical objectivity, which, combined with the complexity of data management and the subordinate position of those taking decisions in an organisation, can make it harder for a human decision-maker to take a decision other than the one suggested by the algorithm*." A. MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasburgo, 25 gennaio 2019, T-PD(2018)09Rev), 10. Cfr. B.D. MITTELSTADT, P. ALLO, M. TADDEO, S. WACHTER, L. FLORIDI, *The ethics of algorithms: Mapping the debate*, *Big Data & Society*, 2, 2016, 1ss; R. CARUANA, Y. LOU, J. GEHRKE, P. KOCH, M. STURM, N. ELHADAD, *Intelligible models for healthcare. Predicting pneumonia risk and hospital 30-day readmission* (21st Annual SIGKDD International Conference on Knowledge Discovery and Data Mining, 2015), 1721-1730.

[267] In questo senso si è espresso anche il Consiglio d'Europa, il quale nelle sue *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in the World of Big Data*, adottate il 27 gennaio 2017 (T-PD(2017)01), al principio 7.4 stabiliva che i decisori umani dovrebbero vedersi riconosciuta la libertà di non fare affidamento sui risultati della determinazione assunta con l'ausilio dei *Big Data*. Cfr. Comitato consultivo della Convenzione sulla protezione delle persone rispetto al trattamento

trattamento automatizzato alla base della decisione potrebbe essere stato condotto sulla base di dati errati, incompleti o non rappresentativi[268]. Specialmente in quest'ultimo caso, peraltro, si pongono gravi rischi di discriminazione dovuti a fenomeni di *intrinsic bias* nella selezione dei dati che hanno "addestrato" l'algoritmo che ha preso la decisione[269].

Alla luce di queste considerazioni, è allora forse comprensibile perché, nonostante la dubbiosa formulazione prediletta dal legislatore europeo, l'interpretazione istituzionale

automatizzato di dati a carattere personale (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, (Starsburgo, 25 gennaio 2019, T-Pd(2019)01), § 4; I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 84; L.A. BYGRAVE, *Data privacy law: an international perspective*, Oxford University Press, Oxford, 2014, 158 ss; C. KUNER, D.J.B. SVANTESSON, F.H. CATE, O. LYNSKEY, C. MILLARD, *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, 7, *Int. Data Priv. Law*, 1, 2017, 1 ss.

[268] A tal proposito, il Comitato consultivo della Convenzione 108 ha messo in guardia circa il rischio della c.d. "decontestualizzazione" di dati e modelli. Tale fenomeno ricorre quando modelli originariamente progettati per una specifica applicazione, sono poi impiegati in diversi contesti o per diverse finalità. COMITATO CONSULTIVO DELLA CONVENZIONE SULLA PROTEZIONE DELLE PERSONE RISPETTO AL TRATTAMENTO AUTOMATIZZATO DI DATI A CARATTERE PERSONALE (Convenzione 108), *Guidelines on Artificial Intelligence and Data Protection*, (Starsburgo, 25 gennaio 2019, T-Pd(2019)01), § 5. Cfr. R. CAPLAN, J. DONOVAN, L. HANSON, J. MATTHEWS, Algorithmic Accountability: A Primer (Data Society Net, 18 aprile 2018) disponibile all'indirizzo www.datasociety.net; ALESSANDRO MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 25 January 2019, T-PD(2018)09Rev), 12. Da notare, peraltro, che già nel 1992 la Commissione delle Comunità europee avvertiva che "The danger of the misuse of data processing in decision-making may become a major problem in future: the result produced by the machine, using more and more sophisticated software, and even expert systems, has an apparently objective and incontrovertible character to which a human decision-maker may attach too much weight, thus abdicating his own responsibilities." COMMISSIONE DELLE COMUNITÀ EUROPEE, Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Bruxelles, 15 ottobre 1992(COM (92) 422 fin.-SYN 287), 26.

[269] Nelle parole del Gruppo di lavoro articolo 29: "[l]a profilazione può perpetuare stereotipi e la segregazione sociale. Può anche confinare una persona in una categoria specifica e limitarla alle preferenze suggerite per tale categoria. Ciò può minare la libertà delle persone di scegliere, ad esempio, determinati prodotti o servizi quali libri, musica o newsfeed. In taluni casi, la profilazione può portare a previsioni imprecise, in altri al diniego di servizi e beni e a discriminazioni ingiustificate." GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017 (Versione emendata e adottata in data 6 febbraio 2018 dallo EDPB) (WP 251 rev.01), 6. Cfr. E. FRONZA, C. CARUSO (a cura di), Ti faresti giudicare da un algoritmo? Intervista ad Antoine Garapon, 4, Questione Giustizia, 2018, 196 ss; D.LEWANDOWSKI, Is Google Responsible for Providing Fair and Unbiased Results?, in M. TADDEO, L. FLORIDI (a cura di), The Responsibilities of Online Service Providers, Law, Governance and Technology Series, Vol. 31, Springer, New York, 2017, 62; A. OTTOLIA, *Big Data* e Innovazione Computazionale, Quaderni di Aida n.28, Torino, Giappichelli Editore, 2017, 6 ss; M. RHOEN, Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, International Data Privacy Law, 2, 2018, 140 ; T. CALDERS, I. ŽLIOBAITĖL, Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures, in B. CUSTERS, T. CALDERS, B. SCHERMER, T. ZARSKY (a cura di), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer, New York, 2013, 43 ss. Sul punto si veda meglio infra nel terzo paragrafo del presente capitolo.

e dottrinale prevalente preferisca riconoscere nell'articolo 22 GDPR un divieto generale, la cui operatività prescinde dal coinvolgimento attivo del soggetto interessato[270].

A conclusione di questa ricognizione del contesto tecnico-informatico e dei prodromi legislativi in cui si è venuto ad inserire l'articolo 22 GDPR, e a riprova della sua rinnovata attualità a livello internazionale, si richiamano i due più recenti avanzamenti registrati dalla norma oggetto del presente capitolo a livello sovra-europeo.

Il primo è rappresentato dal nuovo articolo 9 della Convenzione modernizzata sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (c.d. Convenzione 108+)[271]. Adottato il 18 maggio 2018 dal Consiglio d'Europa, infatti, il protocollo di modifica ha introdotto il diritto di ogni individuo di non essere soggetto ad una decisione esclusivamente automatizzata che incide significativamente sulla propria sfera giuridica, senza che gli venga garantita la possibilità di esprimere la propria opinione[272]. Vale la pena notare, tuttavia, che nella relazione esplicativa della Convenzione 108+, il Comitato *ad hoc* per la protezione dei dati ha specificato che, in virtù del nuovo articolo 9, i soggetti interessati hanno il diritto di contestare la decisione automatizzata, esponendo la propria opinione[273]. Tale interpretazione della disposizione potrebbe suscitare il sospetto che, a differenza del GDPR, la Convenzione 108+ si sia limitata a riconoscere un diritto attivo di opposizione, evitando di fissare un divieto generale di trattamento unicamente automatizzato dei dati a fini decisionali.

[270] Nello stesso senso si collocano anche le parole dello European Data Protection Supervisor, per cu: "[i]nterpretare l'articolo 22 come un divieto piuttosto che come un diritto da invocare significa che le persone sono automaticamente protette dagli effetti potenziali che questo tipo di trattamento può avere." EUROPEAN DATA PROTECTION SUPERVISOR, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit*, 11 aprile 2017, 21-22.

[271] La versione emendata della Convenzione, ratificata dall'Italia il 5 marzo 2019, l'unico trattato internazionale deputato a fissare principi vincolanti a livello internazionale sul tema. Prima delle modifiche apportate dal Consiglio d'Europa, infatti, la Convenzione 108 contava più di 50 Stati membri. Cfr. CONSIGLIO D'EUROPA, *Enhancing data protection globally: Council of Europe updates its landmark convention* (Elsinore, 18 maggio 2018) disponibile all'indirizzo <coe.int/directorate_of_communications>.

[272] Convenzione modernizzata sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, adottata il 16 maggio 2018 in occasione della 128esima Sessione del Comitato dei Ministri del Consiglio d'Europa, Elsinore, Danimarca (CM/Inf(2018)15-final).

Nello stesso senso si era precedentemente espresso anche il Consiglio d'Europa nella sue *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in the World of Big Data*, adottate il 27 gennaio 2017 (T-PD(2017)01).

[273] AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), *Explanatory Report of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) (128esima Sessione del Comitato dei Ministri, Elsinore 17-18 maggio 2018), §75.

Pochi mesi dopo l'adozione della Convenzione 108+, peraltro, nell'ambito della quarantesima conferenza internazionale dei commissari per la protezione dei dati e della privacy, una disposizione simile è confluita nella "Dichiarazione sull'etica e la protezione dei dati nell'Intelligenza Artificiale". Dalla lettura dell'atto, si evince come questa promuova il rafforzamento della posizione dei soggetti interessati, tra l'altro, riconoscendogli il diritto di opporsi all'utilizzo di tecnologie suscettibili di influenzare lo sviluppo delle proprie opinioni e garantendogli, ove applicabile, il diritto di non essere soggetti a decisioni automatizzate che producono effetti significativi sulla propria sfera giuridica. Interessante, anche qui, come la dichiarazione specifichi che, nel caso in cui tale diritto non sia applicabile, i soggetti interessati debbano comunque vedersi garantito il diritto di contestare tali decisioni[274].

Dimostrato, quindi, il ruolo strategico del principio di diritto fissato (a livello europeo) nell'articolo 22 GDPR, e sposata la tesi della sua natura di divieto generale, l'indagine proseguirà con la disamina dei molteplici presupposti di operatività della disposizione, nonché delle sue eccezioni.

2.2. Gli elementi costitutivi della fattispecie

Uno dei motivi generalmente addotti a giustificazione della scarsa operatività dell'articolo 22 GDPR è la molteplicità degli elementi fissati dalla norma ai fini della sua operatività[275]. Affinché sia integrata la fattispecie ivi disciplinata, infatti, è necessario che ricorrano congiuntamente i seguenti presupposti: (i) la decisione sia "basata unicamente sul trattamento automatizzato, compresa la profilazione"[276]; (ii) la decisione così presa nei confronti del soggetto interessato "produca effetti giuridici che lo riguardano o […] incida in modo analogo significativamente sulla sua persona"[277]; (iii) la decisione non sia "necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare

[274] *COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Cnil), EUROPEAN DATA PROTECTION SUPERVISOR (EDPS), GARANTE PER LA PROTEZIONE DEI DATI PERSONALI*, Declaration on Ethics and Data Protection in Artifical Intelligence *(40esima Conferenza internazionale dei commissari per la protezione dei dati e per la privacy, 23 ottobre 2018, Bruxelles), § 5.C.*

[275] A tal proposito, Mendoza parla della disposizione come di una "*house of cards*". I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 82.

[276] Articolo 22, co. 1 GDPR.

[277] Articolo 22, co.1 GDPR.

del trattamento"[278]; (iv) la decisione non sia "autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare"[279]; e, infine, (v) la decisione non sia basata sul consenso esplicito dell'interessato[280].

Al fine di favorire una più organica percezione della fattispecie presa in considerazione dal legislatore europeo nell'articolo 22 GDPR, il prosieguo della trattazione tenterà di sciogliere, uno ad uno, i vari quesiti interpretativi posti da ciascuno dei presupposti di operatività della norma.

2.2.1. Il trattamento "unicamente" automatizzato

La prima modifica introdotta nel 2016 ha riguardato l'estensione del campo di applicazione del previgente articolo 15 Dir. 95/46/CE. Il perimetro di operatività dell'articolo 22 GDPR, infatti, non è più limitato ai trattamenti automatizzati "destinati a valutare taluni aspetti della […] personalità"[281], e quindi esclusivamente alla c.d. profilazione[282], ma raggiunge più genericamente qualsiasi "processo decisionale automatizzato relativo alle persone fisiche, *compresa* la profilazione"[283].

Da notare, tuttavia, che questa affermazione non è esente da obiezioni. Parte della dottrina, infatti, ritiene che il trattamento automatizzato a cui fa riferimento la disposizione debba intendersi come una condizione necessaria della profilazione.

[278] Articolo 22, co.2 lett. a GDPR.
[279] Articolo 22, co.2 lett. b GDPR.
[280] Articolo 22, co.2 lett. c GDPR.
[281] Così recita l'articolo 15, comma 1 Direttiva 95/46/CE del Parlamento Europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, G.U.C.E. L. 218/31. Cfr. L. DURST, *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, cit., 58 ss.
[282] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, Torino, 2016, 193 ss; I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 90ss; A. D'AGOSTINO, *Il sistema di gestione della privacy*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 35 ss; A. NERVI, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 164 ss.
[283] Questa la rubrica del nuovo articolo 22 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE G.U. L119/1 (corsivo aggiunto).

Sebbene questa impostazione renderebbe superflua la nuova formulazione nella parte in cui menziona il trattamento unicamente automatizzato, i sostenitori di questa posizione ritengono che ciò sia più conforme allo spirito della disposizione. A supporto di tale soluzione ermeneutica si allega la circostanza per cui, nel corso nei lavori preparatori, l'enfasi venne posta in via quasi esclusiva sugli effetti pregiudizievoli della profilazione. Di conseguenza, ritenere la profilazione una mera tipologia di trattamento automatizzato amplierebbe in modo ingiustificato la sfera di operatività del divieto, compromettendo lo sviluppo di trattamenti unicamente automatizzati del tutto neutri (*e.g*. il rifiuto di una richiesta di prelevare contante)[284]. È evidente, tuttavia, che il dato testuale rende quantomeno forzata una tale operazione interpretativa, rendendola difficilmente condivisibile.

L'articolo 4 GDPR, infatti, ispirandosi alla nozione precedentemente elaborata dal Consiglio d'Europa[285], ed esplicitando un concetto già implicito nella Direttiva madre, definisce la profilazione come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"[286].

Ne consegue che la profilazione, pur implicando una qualche forma di trattamento automatizzato, presenta delle peculiarità che la rendono più precisamente una

[284] I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 90. In questo senso, già in sede di consultazione circa la formulazione del previgente articolo 15 Dir. 1995/46/CE, la Commissione delle Comunità europee chiariva che "*The processing must apply variables which determine a standard profile (considered good or bad) to the data concerning the data subject; this excludes all cases were the system does not define a personality profile: for example, the fact that a person is unable to obtain the sum of money he wants from an automatic cash dispenser because he has exceeded his credit limit would not fall inside this definition*." COMMISSIONE DELLE COMUNITÀ EUROPEE, *Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Bruxelles, 15 ottobre 1992(COM (92) 422 fin.-SYN 287), 26.

[285] CONSIGLIO D'EUROPA, *La protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione* (Raccomandazione CM/Rec (2010)13 del 23 novembre 2010). Cfr. G. D'IPPOLITO, E.M. INCUITTI, I processi decisionali interamente automatizzati nel settore assicurativo, in *Rivista di diritto dell'impresa*, 3, 2019, 735ss.

[286] Articolo 4, co.1 n. 4 GDPR.

sottocategoria di quest'ultimo[287]. In particolare, la profilazione è un tipo di trattamento dei dati finalizzato alla formulazione di un giudizio che, generalmente, si distingue in tre fasi: la raccolta dei dati, l'analisi per individuare correlazioni, e l'applicazione dei *pattern* così estrapolati ad una persona fisica per valutare o fare previsioni circa la sua capacità di eseguire un compito, i suoi gusti ed interessi, ovvero di anticiparne i comportamenti[288].

Si può quindi affermare che, a differenza dell'articolo 15 Dir. 95/46/CE, il Regolamento, consapevole dei nuovi rischi posti dallo sviluppo tecnologico dell'IA alimentata da *Big Data*, ha ampliato lo scopo di applicazione dell'articolo 22 GDPR, includendo anche forme di trattamento unicamente automatizzato con fini decisionali, ma non deputati a valutare particolari aspetti personali dell'interessato.[289]

Più specificamente, "il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano"[290]. Tali mezzi non necessariamente includono la profilazione, come avviene, ad esempio, nel caso in cui si utilizzino sistemi elettronici di rilevamento della velocità per infliggere multe. Se, tuttavia, l'ammontare della multa fosse parametrato al profilo dell'utente, inferito dal trattamento automatizzato di informazioni ulteriori volte a definirne l'attitudine alla pericolosità alla guida, allora si creerebbe una sovrapposizione fra profilazione e processo decisionale automatizzato[291].

---

[287] Cfr. S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 128 ss; I. DESTRI e A.M. LOTTO, *La profilazione*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 141 ss; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, Torino, 2016, 193 ss.

[288] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 7.

[289] Cfr. G. MARINO, *I diritti degli interessati*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 88; L. SCUDIERO, *Il consenso come condizione di liceità*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 95.

[290] G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243 ss; UK INFORMATION COMMISSIONER'S OFFICE (ICO), *Feedback request- profiling and automated decision-making*, 2017, 19; M. BRKAN, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, 11, *International Journal of Law and Information Technology*, 2019, 1-31.

[291] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento*

Ciò posto, si deve anche precisare che l'articolo 22 GDPR non prende in considerazione qualsiasi trattamento automatizzato, ma soltanto i processi decisionali *unicamente* automatizzati.

Riecheggia, in tal senso, la distinzione di Searle fra *strong* e *weak* AI. Affinché un trattamento possa dirsi unicamente automatizzato, infatti, non è sufficiente che le risultanze ottenute per vie automatizzate vengano utilizzate dall'operatore umano per maturare la propria decisione (*weak* AI), ma è necessario che la decisione stessa sia imputabile all'algoritmo e, solo successivamente, comunicata all'agente umano (*strong* AI)[292].

Il divieto, però, non potrebbe essere eluso attraverso un coinvolgimento umano meramente formale[293]. A tal fine, è stato opportunamente chiarito che una decisione può dirsi unicamente automatizzata non solo qualora manchi totalmente l'intervento umano, ma anche nel caso in cui quest'ultimo sia effettuato da un soggetto che non ha l'autorità e le competenze necessarie ad effettuare una valutazione significativa della decisione assunta dall'algoritmo[294]. In altri termini, prima che la determinazione prodotta in via automatizzata dal sistema informatico sia ufficializzata, deve essere garantito un previo controllo umano da parte di un soggetto idoneo ad incidere sulla sostanza del provvedimento e, eventualmente, modificarlo[295].

2016/679, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 8-9.

[292] J.R. SEARLE, Minds, Brains and Science, 3, *Behavioral and Brain Sciences*, 1980, 3, 417 ss. Sul punto si rinvia a quanto detto *supra* § 2.1 spec. nt. 12.

[293] L'Intelligenza Artificiale deve fornire assistenza ai decisori umani, ottimizzando l'individuazione di match in mercati ad alta intensità di dati. Agli agenti umani, tuttavia, dovrebbe sempre essere rimessa la decisione sull'*an* e il *quantum* della delega operativa da concedere ai sistemi di IA. In questo si è espresso V. MAYER-SCHÖNBERGER e T. RAMGE, *Reiventing Capitalism in the Age of Big Data*, Basic Books, New York, 2018, 12.

[294] A tal proposito si è anche parlato del diritto ad ottenere l'intervento umano come di una diversa declinazione del principio di autodeterminazione. Inteso in senso lato, quest'ultimo giustificherebbe il diritto ad una versione c.d. *non-smart* della fornitura di servizi basati su sistemi di IA. A. MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasburgo, 25 gennaio 2019 (T-PD(2018)09Rev), 8. In senso analogo, il sedicesimo *Asilomar AI Principle*, rubricato "*human control*", stabilisce che "[*h]umans should choose how and whether to delegate decisions to AI systems, to accomplish human-chosen objectives.*" *Asilomar AI Principles*, adottati alla conferenza *Beneficial AI 2017* (Future of life institute, 5-8 gennaio 2017).

[295] EUROPEAN DATA PROTECTION SUPERVISOR, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit*, 11 aprile 2017, 23. Di questo problema si parla anche in termini di "*techno-dependency*". Con tale espressione si indica, infatti, la tendenza a delegare (anche inconsciamente) una serie sempre più ampia di scelte a sistemi informatici, rimettendosi ai

2.2.2. Gli effetti giuridici o altri effetti significativi

Il secondo elemento costitutivo della fattispecie disciplinata dall'articolo 22 GDPR riguarda le conseguenze che la decisione unicamente automatizzata, così come definita nel precedente sotto paragrafo, deve produrre nella sfera giuridica dell'interessato.

A integrazione di quanto statuito nel previgente articolo 15 Dir. 95/46/CE, il legislatore europeo ha specificato la nozione di "effetti significativi" qualificando la relazione che intercorre fra questi ultimi e gli effetti giuridici. In particolare, l'articolo 22 GDPR puntualizza che il divieto ivi fissato opera solo nel caso in cui la decisione automatizzata assunta nei confronti dell'interessato "produca effetti giuridici che lo riguardano o […] incida in modo analogo significativamente sulla sua persona"[296].

Il rapporto di analogia fissato dal legislatore fra quelli che, nella previgente formulazione, erano gli effetti giuridici e quelli significativi, per parte della dottrina è indice del carattere necessariamente non bagatellare dei secondi[297]. Peraltro, sebbene ciò non presupponga la natura pecuniaria delle ripercussioni subite[298], si ritiene che non possano ritenersi "significative" *ex* articolo 22 GDPR conseguenze meramente emotive[299].

La decisione unicamente automatizzata è quindi vietata se, pur non producendo effetti *stricto sensu* giuridici[300], raggiunge conseguenze di "analoga" rilevanza, a

suggerimenti da essi formulati in base al profilo attributo di volta in volta all'utente. Cfr. P. PAŁKA, A. JABŁONOWSKA, H.W. MICKLITZ e G. SARTOR, *Before machines consume the consumers. High-Level Takeaways from the ARTSY Project*, EUI Working papers, 2018 (LAW 2018/12), 13.

[296] G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario. Regolamento (UE) 2016/679 del 27 aprile 2016 - Decreto di adeguamento D.Lgs. n. 101/2018 - Codice privacy D.Lgs. n. 196/2003*, Ipsoa, Milano, 2018, 219 ss.

[297] I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 89.

[298] P. CHURCH, C. MILLARD, Comments on the data protection directive, in A. BÜLLESBACH, S. GIJRATH, Y. POULLET, C. PRINS (a cura di), Concise European IT law, 2 ed., Kluwer Law International, Alphen aan den Rijn, 2010, 84.

[299] I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 90.

[300] Secondo l'interpretazione datane dal Gruppo di lavoro articolo 29, si tratterebbe di decisioni automatizzate che incidono su diritti soggettivi assoluti (quali, ad esempio, il diritto di voto e di agire in giudizio), su diritti soggettivi relativi (come quelli derivanti dalla stipula di un contratto), ovvero su status giuridici del soggetto interessato. Tra queste ipotesi il Gruppo di lavoro articolo 29 annovera la risoluzione di un contratto, la concessione o negazione di una prestazione sociale o della cittadinanza. GRUPPO DI

prescindere dal carattere negativo o meno delle stesse[301]. Come messo in luce dal considerando 71 GDPR, questo potrebbe accadere, ad esempio, nel caso in cui la decisione unicamente automatizzata conduca al rifiuto di una domanda di credito *online* ovvero a pratiche di assunzione elettronica. Si tratta, in linea generale, di fattispecie in cui il processo decisionale automatizzato, pur lasciando impregiudicati diritti e/o gli obblighi dell'interessato, ne condiziona comportamenti e scelte, ha un'incidenza prolungata sullo stesso, ovvero porta alla sua esclusione o discriminazione. Dalla casistica generalmente richiamata, peraltro, si evince che, per raggiungere la soglia di significatività degli effetti giudici, la decisione dovrebbe incidere su circostanze particolari quali l'accesso al credito, a servizi sanitari, all'impiego, all'istruzione, ecc.[302].

In questo senso, si discute se in tale accezione di significatività degli effetti possano rientrare anche le pratiche di c.d. *targeted advertising*[303].

Nel corso dei lavori preparatori al GDPR, il *Rapporteur* del Comitato per gli affari legali, aveva proposto un emendamento alla versione del considerando 58 formulata dalla Commissione. In particolare, Gallo riteneva opportuno specificare che, da un lato, gli effetti prodotti dalla decisione automatizzata dovessero essere necessariamente negativi e che, dall'altro, questi fossero per definizione estranei a pratiche di comunicazione commerciale per la gestione o acquisizione della clientela[304]. È noto, tuttavia, che le

---

LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 23.

[301] A supporto di questa interpretazione viene, ancora una volta, l'argomento sistematico offerto dalla lettura dell'analogo principio fissato dall'articolo 11 Direttiva 2016/680/UE in virtù del quale la decisione unicamente automatizzata, per essere considerata vietata, deve produrre "effetti giuridici negativi o incid[ere] significativamente sull'interessato". Ne discende, quindi, che ove il legislatore europeo avesse voluto restringere il campo di applicazione del divieto alle sole decisioni automatizzate suscettibili di incidere negativamente sulla sfera giuridica dell'interessato, lo avrebbe fatto espressamente. Cfr. L.A. BYGRAVE, Minding the machine: Article 15 of the EC data protection directive and automated profiling, 17, *Comput. Law Secur. Rev*., 1, 2001, 2ss; L.A. BYGRAVE, Data protection law: approaching its rationale, logic and limits, Kluwer Law International, Alphen aan den Rijn, 2002, 322 ss.

[302] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 24.

[303] Cfr. R. PANETTA, *Privacy is not dead: it's hiring*!, in ID. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 30 ss. Per un esempio concreto di c.d. *redlining* in ambito creditizio con conseguenze discriminatorie si veda L. VAUGHAN, *Mapping Society. The Spatial Dimensions of Social Cartography*, UCL Press, 2018, 156 ss.

[304] RAPPORTEUR M. GALLO, *Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Legal Affairs, 23 Marzo 2013), 13-14.

profonde correlazioni che legano le enormi quantità di dati orbitanti nel circuito *Big Data* hanno reso sempre più frequenti gli episodi di *web-lining*[305]. Con questa espressione, si indica l'utilizzo di *proxy data* di informazioni sensibili a fini di profilazione[306].

In linea generale, quindi, si può ritenere che di regola la pubblicità *online* basata su strumenti automatizzati non incida in modo analogo significativamente sui soggetti interessati. È pur vero, però, che in base ad alcune circostanze particolari del caso, le comunicazioni pubblicitarie potrebbero risultare particolarmente invasive (tracciamento su siti, dispositivi e servizi diversi), nonché volte a sfruttare particolari vulnerabilità dei destinatari delle comunicazioni, arrivando anche a differenziare non soltanto le comunicazioni ma anche i prezzi[307].

Infine, potrebbero verificarsi casi in cui il trattamento differenziato del soggetto non derivi da suoi comportamenti, ma da condotte di terzi che vivono nella medesima area geografica o condividono con lui interessi, acquisti o altri tratti comuni. I sistemi di ML, infatti, rendono sempre più agevole prescindere da una dimensione squisitamente individuale del profilo, potendo inferire le caratteristiche e i gusti di un soggetto dalla sua riconducibilità ad un gruppo (più o meno ristretto) di individui che condividono le sue stesse caratteristiche[308].

---

305 M. VERMEULEN, *Regulating profiling in the general data protection regulation: an interim insight into the drafting of Article 20, (*EMSOC project. User empowerment in a social media culture, 1 settembre 2013, Bruxelles*).* Cfr. A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 442 ss.

306 T. MILLER, P. HOWE, L. SONENBERG, *Explainable AI: Beware of Inmates Running the Asylum Or: How I Learnt to Stop Worrying and Love the Social and Behavioural Sciences, ArXiv, 2017, 3;* K. BRENNAN-MARQUEZ, *"*Plausible Cause": Explanatory Standards in the Age of Powerful Machines, *70, Vanderbilt Law Review, 2017, 7;* J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, Accountable Algorithms, *165, University of Pennsylvania Law Review, 2017, 633;* G. AMORE, *Fairness, Transparency e Accountability nella protezione dei dati personali, Studium Iuris, 4, 2020, 414 ss.*

307 Cfr. M. MAGGIOLINO, *Big Data* e prezzi personalizzati, 1, *Concorrenza e mercato*, 2016, 95 ss.

308 Per approfondimenti sul concetto di "*privacy* di gruppo" si veda meglio *infra* nel prossimo paragrafo. Cfr. A. ODDENINO, *Reflection on Big Data and International Law*, 4, *Diritto del Commercio Internazionale*, 2017, 777 ss; M. HILDEBRANDT, The Dawn of a Critical Transparency Right for the Profiling Era, in J. BUS, M. CROMPTON, M. HILDEBRANDT, G. METAKIDES (a cura di), *Digital Enlightenment Yearbook 2012*, IOS Press, Amsterdam, 49; R. TAYLOR, No Privacy Without Transparency, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura si) *Data Protection and Privacy: The Age of Intelligent Machines,* Hart Publishing, Oxford, 2017, 96; A. MANTELERO, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, 32, *Computer Law & Security*, 2016, 238; L. KAMMOURIEH, T. BAAR, JOS BERENS, E. LETOUZÉ, J. MANSKE, J. PALMER, D. SANGOKOYA, e P. VINCK, Group Privacy in the Age of *Big Data*, in L. TAYLOR, L. FLORIDI, B. SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 43.

In questo modo, tuttavia, si pone con maggiore forza l'esigenza di salvaguardare le persone fisiche da discriminazioni che potrebbero discendere da una personalizzazione non solo degli annunci, ma anche dei prezzi dei prodotti offerti[309].

A dispetto delle pressanti esigenze di tutela sottese alla norma espressa dall'articolo 22 GDPR, fin qui brevemente richiamate, la già fortemente condizionata sfera di operatività della disposizione viene ad essere ulteriormente contratta dalle eccezioni che il secondo paragrafo disciplina rispetto al divieto generale di processi decisionali unicamente automatizzati. È quindi all'analisi di questo secondo aspetto dell'ambito di applicazione dell'articolo 22 GDPR che verrà dedicato il prossimo paragrafo, al fine di completare la panoramica delle caratteristiche che contraddistinguono la fattispecie disciplinata dalla disposizione.

2.3. Le eccezioni al divieto: consenso, necessità e legge

A differenza del previgente articolo 15 co.2 Dir. 1995/46/CE, il nuovo articolo 22, co.2 GDPR riconosce ai soggetti interessati la possibilità di neutralizzare il divieto di essere sottoposti a processi decisionali automatizzati prestando il proprio consenso esplicito[310].

La *ratio* sottostante la deroga consensuale introdotta nel 2016 risponde alla stessa logica ispiratrice che ha mosso, dapprima, il progetto di riforma della Direttiva sulla protezione dei dati personali e, più recentemente, la proposta di regolamento sulla vita privata e le comunicazioni elettroniche in abrogazione dell'ancora vigente Direttiva

[309] S.F. GIOVANNANGELI, L'informativa agli interessati e il consenso al trattamento, in R. PANETTA (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018, Milano, Giuffré, 2019, 128 ss. Cfr. COMMISSIONE DELLE COMUNITÀ EUROPEE, Amended proposal for a Council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Bruxelles, 15 ottobre 1992(COM (92) 422 fin.-SYN 287), 26-27. Per una più approfondita disamina delle questioni giuridiche poste dall'utilizzo dei Big Data a fini di personalizzazione di prezzi e offerte v. AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI, GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Indagine conoscitiva sui Big Data (10 febbraio 2020), 105 ss.

[310] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE G.U. L119/1, articolo 22, co.2, lett. c. Cfr. A.C. NAZZARO, P*rivacy, smart cities e smart cars*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 336 ss; 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*, Cedam, Padova, 2019, 59 ss.

2002/58/CE (d'ora in avanti Regolamento *ePrivacy*)[311]: rafforzare la capacità dei soggetti interessati di esercitare un controllo effettivo sui propri dati personali.

In questo senso, si è più volte espresso il Gruppo di lavoro articolo 29, ribadendo come, da un lato, "[s]e usato correttamente, il consenso rappresent[i] uno strumento che offre all'interessato una forma di controllo sul trattamento dei dati che lo riguardano", mentre dall'altro, "[s]e utilizzato in maniera errata, […] [sia] soltanto illusorio e […] un fondamento inadeguato per legittimare il trattamento"[312].

La base giuridica del consenso, infatti, è tradizionalmente ricondotta alla tutela del diritto all'autodeterminazione dei soggetti interessati, in molti Stati membri spesso ritenuta espressione di principi di matrice costituzionale[313]. Tale premessa teleologica spiega, peraltro, il *favor* mostrato dal legislatore europeo in sede di riforma della Direttiva 2002/58/CE (d'ora in avanti Direttiva *ePrivacy*), in occasione della quale il Gruppo di lavoro articolo 29 ha riaffermato la prevalenza, in materia di tutela dei dati personali nelle comunicazioni elettroniche, del consenso sulle altre basi giuridiche[314].

Sebbene il ruolo cruciale del consenso in materia di protezione dei dati personali sia, in termini più generali, confermato anche dal disposto degli articoli 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea[315], il GDPR, sul solco della previgente

[311] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), adottata a Bruxelles il 10 gennaio 2017 (COM(2017) 10 final).

[312] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE, adottato il 9 aprile 2014 (844/14/IT), 19. Tale affermazione è stata poi ribadita nel 2018, in occasione dell'adozione delle linee guida sul consenso che, in virtù dell'evoluzione di tale base giuridica di trattamento dei dati, sono intervenute ad integrare i principi, pur sempre attuali e non sostituiti, dettati dal Gruppo di lavoro articolo 29 nel parere 15/2011 sulla definizione di consenso. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 3. Cfr. M. MASSIMI, Quali orizzonti per il marketing?, in R. PANETTA (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018, Milano, Giuffré, 2019, 486 ss.

[313] Così GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 15/2011 on the definition of consent*, adottato il 13 luglio 2011 (WP187), 7ss. Sul "diritto fondamentale all'autodeterminazione, in cui si realizza il valore fondamentale della dignità umana, sancito dall'art. 32 Cost., dagli art. 2, 3 e 35 della Carta dei diritti fondamentali dell'Unione europea e dalle convenzioni internazionali", sviluppato principalmente con riguardo al diritto del paziente di rifiutare le cure mediche, si veda ex multis, e da ultimo, Cass. civ. Sez. I Ord., 15 maggio 2019, n. 12998.

[314] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*, adottata il 16 luglio 2016 (WP 240), 4.

[315] P.F. GIUGGIOLI, Tutela della privacy e consumatore, in E. TOSI (a cura di), Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, Giuffré, 2019, 273;

Direttiva 1995/46/CE[316], continua a considerare il consenso "uno dei vari motivi che legittimano il trattamento dei dati personali, anziché il fondamento giuridico principale"[317].

Ciò discende dalla circostanza per cui, al ricorrere di determinati presupposti fattuali, spesso tipici dell'ecosistema digitale, il consenso dei soggetti interessati viene svuotato della sua effettività al punto tale da rendere inadeguata la tutela da esso apprestata[318]. Al fine di meglio sostanziare tale affermazione, e sebbene la disamina delle innumerevoli questioni giuridiche sollevate dal consenso esuli dallo scopo del presente capitolo, è comunque opportuno procedere ad una rapida, seppur puntuale, descrizione dei requisiti che il consenso deve rispettare per potersi qualificare come una adeguata base giuridica ai sensi dell'articolo 22, co.2 lett. c GDPR.

La fattispecie della prestazione di un consenso esplicito ai fini dell'adozione di decisioni unicamente automatizzate, infatti, deve essere ricostruito alla luce della più generica nozione di consenso quale base giuridica per il trattamento dei dati personali *ex* artt. 6(1)(a) e 9(2)(a) GDPR[319]. In particolare, l'articolo 4 co.1 n. 11 GDPR definisce il consenso come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento"[320].

C. BASUNTI, La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali, *Contratto e impresa*, 2, 2020.

[316] Cfr. V. RICCIUTO, *L'economia della privacy. Circolazione dei dati personali e mercato*, cit., 311 ss; V. F. BRAVO, *Il consenso e le altre condizioni di liceità,* in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati*, Zanichelli, Bologna, 2017, 101 ss.

[317] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014 (844/14/IT), 19. Cfr. A.C. NAZZARO, P*rivacy, smart cities e smart cars*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 336 ss.

[318] Cfr. F. CAGGIA, *Libertà ed espressione del consenso*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 264 ss; E. LUCCHINI GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 71 ss.

[319] I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 94.

[320] Cfr. L. SCUDIERO, *Il consenso come condizione di liceità*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 95 ss.

Affinché possa assurgere a reale espressione di volontà (*rectius* di controllo), il consenso dovrebbe quindi essere innanzitutto libero. In altri termini, la manifestazione di volontà con cui il soggetto interessato acconsente al trattamento dei suoi dati personali, non deve risultare il prodotto, neppure indiretto, di una qualsivoglia azione di pressione o influenza inappropriata[321].

Come puntualizzato dal considerando 43 GDPR, ciò potrebbe verificarsi nel caso in cui sussista un c.d. "evidente squilibrio" tra il titolare del trattamento e il soggetto interessato[322]. Specificando ulteriormente la fattispecie, il considerando declina tale asimmetria in termini di dipendenza. Si esclude, quindi, a titolo esemplificativo, che il consenso possa configurare un'idonea base giuridica ove il titolare del trattamento sia un'autorità pubblica[323], ovvero il datore di lavoro del soggetto interessato[324]. In tali circostanze, prosegue il legislatore, la posizione di fisiologica debolezza dell'interessato, rende "improbabile" riconoscere nella prestazione del consenso quel grado di libertà

[321] In altri termini, il consenso non è libero nella misura in cui e "frutto di "tecniche commerciali aggressive o suggestive", turbato da "disorientamenti, stratagemmi, opacità, sotterfugi, slealtà, doppiezze o malizie comunque adottate dal titolare del trattamento". S. THOBANI, Protezione dei dati personali. Operazioni di *tying* e libertà del consenso, 3, *Giur. It.*, 2019, 530 ss. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 6; G. RESTA, V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, 2, *Rivista Trimestrale di Diritto e Procedura Civile*, 2018, 411 ss; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Edizioni Scientifiche Italiane, Napoli, 2017, 72 ss.

[322] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, 113 ss.

[323] Per tale ipotesi il Gruppo di lavoro articolo 29 indicava, quali più idonee basi giuridiche, quelle di cui all'articolo 6 co.1 lett. c ed e, ovvero, rispettivamente, la necessità del trattamento per l'esecuzione di un contratto (o di misure precontrattuali) e la necessità del trattamento "per l'esecuzione di compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento." Nello stesso senso si esprime il considerando 31 GDPR, il quale specifica che "[l]e autorità pubbliche a cui i dati personali sono comunicati conformemente a un obbligo legale ai fini dell'esercizio della loro missione istituzionale, quali autorità fiscali e doganali, unità di indagine finanziaria, autorità amministrative indipendenti o autorità dei mercati finanziari, responsabili della regolamentazione e della vigilanza dei mercati dei valori mobiliari, non dovrebbero essere considerate destinatari qualora ricevano dati personali che sono necessari per svolgere una specifica indagine nell'interesse generale, conformemente al diritto dell'Unione o degli Stati membri." Sul concetto di necessità, si veda meglio *infra* nel presente paragrafo. Cfr. G. BIFERALI, *Big Data* e valutazione del merito creditizio per l'accesso al *peer to peer lending*, 3, *Diritto dell'informazione e dell'informatica*, 2018, 487 ss.

[324] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 15/2011 on the definition of consent*, adottato il 13 luglio 2011 (WP187), 13-15; GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI , *Opinion 8/2001 on the processing of personal data in the employment context*, adottata il 13 settembre 2001 (WP 48) (5062/01/EN/Final), 23 ss; GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI , *Working document on the surveillance of electronic communications in the workplace*, adottato il 29 maggio 2002, (WP 55) (5401/01/EN/Final), 21 ss; GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI , Opinion 2/2017 on data processing at work, adottata l'8 giugno 2017, (WP 249) (17/EN), 23 ss; M. DE BERNART, *La videosorveglianza e il controllo del lavoratore*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 543 ss.

necessario a renderla un'idonea base giuridica. Da tali considerazioni, tuttavia, il legislatore europeo non ha ritenuto di far discendere la radicale invalidità del consenso prestato ma, più pragmaticamente, l'introduzione di una presunzione semplice con conseguente onere di prova contraria in capo al titolare del trattamento[325].

I lavori preparatori al GDPR, peraltro, mostrano come queste preoccupazioni fossero particolarmente sentite dalla Commissione europea, la quale le aveva fatte confluire nella proposta di testo dell'articolo 7 co.4 del GDPR, il quale avrebbe dovuto sancire un vero e proprio divieto di avvalersi della base giuridica del consenso in tali ipotesi. In senso analogo, il Comitato per le libertà civili, la giustizia e gli affari interni, aveva proposto di specificare ulteriormente la formulazione adottata dalla Commissione per l'allora considerando 34 (oggi considerando 43), includendo fra le esemplificazioni di squilibrio, l'ipotesi in cui il titolare del trattamento detenga un potere di mercato significativo rispetto a determinati prodotti o servizi e ne condizioni l'offerta alla prestazione del consenso, ovvero, modificando unilateralmente le condizioni del rapporto, interferisca col godimento del servizio, mettendo l'interessato nella condizione di dover scegliere tra acconsentire al trattamento dei propri dati, ovvero perdere i risultati del tempo investito nella risorsa *online* (e.g. nella creazione di un profilo di *social network*)[326].

Più scettica, invece, la posizione del Comitato per il mercato interno e la protezione dei consumatori, il quale giudicava troppo radicale la previsione di un divieto assoluto di prestazione del consenso in caso di squilibrio di potere fra le parti. Ciò in quanto, in tal modo, sosteneva il Comitato, si sarebbe preclusa all'interessato la possibilità di prestare il consenso anche nel caso in cui il trattamento dei dati fosse stato

[325] Tale soluzione, ha osservato il Gruppo di lavoro articolo 29, risponderebbe alla finalità di responsabilizzazione dei titolari del trattamento, che caratterizza una delle principali ratio ispiratrici del GDPR. Sulla finalità di responsabilizzazione delle imprese si veda anche A. D'AGOSTINO, *Il sistema di gestione della privacy*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, cit, 31 ss.

[326] RAPPORTEUR M. GALLO, *Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Legal Affairs, 23 Marzo 2013), 6.

nel suo interesse, e avesse mantenuto la possibilità di revocarlo in ogni momento, senza subire alcun pregiudizio[327].

Il compromesso fra le due opposte posizioni è risultato nel totale silenzio dell'articolo 7 GDPR sul punto, e nella degradazione del divieto a presunzione semplice, nonché nella sua esclusiva menzione al solo più debole livello interpretativo offerto dai considerando[328].

Ai sensi dell'articolo 4 co.1 n.11 GDPR il consenso, per assurgere a presupposto legittimo per il trattamento dei dati personali, e quindi, *a fortiori*, per legittimare l'adozione di decisioni unicamente automatizzate nei suoi confronti, deve rispettare un secondo requisito: la specificità.

In particolare, un consenso specifico è innanzitutto un consenso c.d. granulare, ossia un consenso prestato separatamente per ciascuna delle diverse finalità eventualmente perseguite dal titolare attraverso un unico trattamento dei dati. Questo potrebbe essere il caso, ad esempio, di un rivenditore *online* che presenta un'unica richiesta di consenso al trattamento dei dati personali del cliente sia per inviare

[327] A fini esemplificativi, veniva menzionato il caso in cui il datore di lavoro chiedeva il consenso al trattamento dei dati personali del proprio dipendente per offrirgli una copertura assicurativa. RAPPORTEUR LARA COMI, *Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 28 gennaio 2013, 411-412. In senso analogo si è recentemente espressa quella parte della dottrina che ritiene di dover guardare all'interesse del soggetto interessato nel valutare la libertà o meno del consenso prestato, con conseguente presunzione di validità dello stesso nel caso in cui la decisione automatizzata presa vada in suo favore. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017, 94. Cfr. M. FRAIOLI, *Il diritto di opposizione e la revoca del consenso*, S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 242 ss.

[328] Cfr. 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*, Giappichelli Editore, Torino, 2019, 10 ss; F. PIRAINO, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, 2, *Nuove leggi civ. comm.*, 2017, 369 ss; A. RICCI, Sulla "funzione sociale" del diritto alla protezione dei dati personali, cit., 586 ss; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, 109 ss.

comunicazioni pubblicitarie, che per trasmettere gli stessi ad altri *partner* del medesimo gruppo[329].

In secondo luogo, un consenso è specifico se preceduto da una chiara e puntuale descrizione di ciascuna delle diverse finalità del trattamento per cui viene chiamato ad acconsentire in modo granulare. Il requisito della specificazione delle finalità[330], peraltro, presenta una stretta affinità con il principio di limitazione delle finalità, ponendosi, anzi, allo stesso tempo, come condizione di specificità del consenso e come misura di prevenzione e contrasto al fenomeno dell'"ampliamento progressivo, o [del]la commistione, delle finalità di trattamento dei dati dopo che l'interessato ha acconsentito alla loro raccolta iniziale" (c.d. *function creep*)[331]. Ai sensi dell'articolo 5 co. 1 lett. b GDPR, infatti, i dati personali dell'interessato devono essere raccolti per finalità "determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità"[332]. In quest'ottica, il riconoscimento del diritto di prestare il proprio consenso in modo specifico (*rectius* separato) per ciascuna finalità di trattamento, prima che questo abbia inizio, consente anche una più accurata verifica della compatibilità di eventuali ulteriori (e successive) finalità con quelle originariamente illustrate all'interessato[333].

[329] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 11. Lo stesso considerando 43 puntualizza come "[s]i presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso."

[330] Cfr. G. CRISTOFARI, *Il diritto alla limitazione del trattamento*, in S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 217 ss.

[331] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 13. Cfr. A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli Editore, Torino, 2018, 89 ss.

[332] GRUPPO DI LAVORO ARTICOLO 29, *Opinion 03/2013 on purpose limitation*, adottata il 2 aprile 2013 (00569/13/EN), 15 ss. Cfr. G. D'IPPOLITO, Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. il caso dell'uso secondario di *Big Data*, 6, *Diritto dell'informazione e dell'informatica*, 2018, 943 ss.

[333] Più specificamente, a tal fine si dovrebbe prendere in considerazione: (i) il rapporto tra le finalità per cui i dati personali sono stati originariamente raccolti e le ulteriori finalità sopravvenute; (ii) il tipo di servizio in occasione della fruizione del quale l'interessato ha prestato il proprio consenso, e le conseguenti ragionevoli aspettative che quest'ultimo poteva maturare circa le finalità perseguite dalla controparte in sede di trattamento dei propri dati personali; (iii) la natura dei dati raccolti; (iv) le conseguenze che l'ulteriore trattamento potrebbe determinare per l'interessato; (v) la misure di salvaguardia che accompagnano il perseguimento delle nuove finalità, al fine di evitare ogni impatto indebito per l'interessato. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo*

Infine, il consenso non è qualificabile come specifico se l'informativa sulle finalità del trattamento, che precede la sua prestazione, non è chiaramente distinta dalle informazioni concernenti altre questioni. Ogni richiesta di consenso, quindi, dovrebbe essere anticipata da una descrizione chiara ed esaustiva delle caratteristiche e delle conseguenze collegate esclusivamente alla particolare finalità del trattamento per la quale viene chiesto al cliente di acconsentire. Ciò implica, ad esempio, che non costituisce un consenso specifico al trattamento dei dati, quello prestato con la stessa azione con cui l'interessato ha aderito alle condizioni generali del servizio offerto dal titolare del trattamento[334].

Tale ultima condizione di specificità del consenso, peraltro, nella misura in cui mira a rendere l'interessato più consapevole delle ricadute che ogni singola prestazione di consenso è suscettibile di produrre sulla propria sfera giuridica, è strettamente collegata al terzo requisito fissato dall'articolo 4 GDPR, ossia quello del carattere informato del consenso[335]. In altri termini, affinché il consenso prestato risulti valido, il titolare del trattamento non può limitarsi a fornire all'interessato informazioni separate e puntuali

decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 12.

[334] Cfr. A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1192 ss. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 18.

[335] Seppure con specifico riferimento alla relazione medico-paziente, è stato osservato che "L'espressione consenso informato, […] rappresenta «un sintagma non scindibile», nella misura in cui il consenso, che deve essere libero e consapevole, non può andare disgiunto da un obbligo informativo a carico del medico, che è strumentale al superamento delle asimmetrie informative tra i protagonisti della relazione terapeutica. Tuttavia, tale locuzione, che fornisce indubbiamente un'efficace sintesi non coglie appieno la complessità ermeneutica che si cela nelle parole che la compongono, essendo il frutto di un processo di imitazione linguistica nell'ambito del diritto che si è sostanziata in una forma di «circolazione dei modelli giuridici». Il concetto di "*informed consent*", elaborato dalla giurisprudenza statunitense, «è infatti stato semplicemente trasposto in italiano e traslitterato in modo grossolano ed ambiguo nella locuzione consenso informato», dovendo invece, più propriamente, tradursi con la dizione "informazione per il consenso" «nel rispetto non solo concettuale ma sicuramente per una decifrazione più corretta ed una interpretazione più precisa in rapporto ai notevoli concetti che presuppone e racchiude». In questo senso S. ROSSI, Consenso informato (voce), *Digesto*, sez. civ., VII, Torino, Utet, 2012, 177 ss. Cfr. G. GENNARI, Consenso informato: ritorno all'anno zero, 71, *Responsabilità civile e previdenza*, 9, 2006, 9, 1411 ss; in senso critico sulla locuzione di consenso informato M. GORGONI, La "stagione" del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione, 64, *Responsabilità civile e previdenza*, 1, 1999, 488 ss; S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 119 ss; F. GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1231 ss

circa le varie finalità di trattamento per cui è chiamato ad acconsentire[336]. In tal modo, infatti, il consenso ottenuto sarebbe sì specifico, ma non informato, in quanto il soggetto interessato non sarebbe posto nella condizione di poter valutare in modo pienamente consapevole le conseguenze della propria scelta[337]. Per questo motivo, in ossequio ai doveri informativi disciplinati dagli articoli 13 e 14 GDPR, espressione del più generico principio di trasparenza, correttezza e liceità del trattamento, il soggetto interessato dovrebbe quantomeno essere edotto circa: (i) l'identità del titolare del trattamento; (ii) le tipologie di dati raccolti ed analizzati; (iii) l'esistenza del diritto di revocare il consenso[338]; (iv) l'esistenza di un processo decisionale automatizzato alimentato da tali dati; nonché, se del caso, (v) la misura dei rischi legati alla possibilità di operare un trasferimento dei suoi dati[339].

Sebbene il GDPR abbia omesso di disciplinarne i requisiti di forma, l'esigenza di tutela perseguita con la previsione di tali obblighi informativi sarebbe destinata a rimanere lettera morta nella misura in cui, nell'adempiere al suo dovere di *disclosure*, la formulazione adottata dal titolare del trattamento non raggiunga quella soglia minima di comprensibilità necessaria a rendere tali informazioni fruibili per una persona media. A tal fine, è fondamentale garantire l'utilizzo di un linguaggio sintatticamente chiaro, linguisticamente accessibile, contenutisticamente esaustivo e sintetico[340]. Sul punto, interessanti sono le riflessioni in tema di c.d. *smart disclosure*, intesa come la predisposizione di moduli informativi a più livelli e integrati in modo interattivo nella fornitura del servizio[341]. In tal modo, sarebbe quindi possibile fornire all'utente

[336] Sui presupposti "equipollenti" delle basi giuridiche per il trattamento dei dati personali si veda, ad esempio, R. PANETTA, *Privacy is not dead: it's hiring!*, in ID. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 20 ss.

[337] R. MESSINETTI, *Circolazione dei dati personali e autonomia privata*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, 142 ss.

[338] Così prevede espressamente l'articolo 7 co. 3 GDPR.

[339] In questo stesso senso si esprime il considerando 42 GDPR, statuendo che "[a]i fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali." Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 14. Cfr. E. LUCCHINI GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 78 ss.

[340] Per lo sviluppo di precipui *Key Performance Indicator* si veda *infra* nel prossimo paragrafo.

[341] Cfr. O. BEN-SHAHAR, C.E. SCHNEIDER, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, Princeton University Press, Princeton, 2014, 55ss; F.H. CATE, *Big Data* consent and the future of data protection in C.R. SUGIMOTO, H.R. EBIKA, M.MATTIOLI (a cura di), *Big Data is not a Monolith*, MIT Press, Cambridge (MA), 2016, 3; M. HILDEBRANDT, The Dawn of a Critical Transparency

informazioni più pertinenti alla sua personale esperienza di utilizzo del servizio, nonché più assimilabili, poiché trasmesse in modo più graduale, evitando così il noto fenomeno dell'*information overload*, all'origine del problema della c.d. fallacia del consenso[342].

Data la forte incidenza che, come si vedrà meglio nel prossimo paragrafo, i processi decisionali *ex* art. 22 GDPR possono avere sulla sfera giuridica dei destinatari, il legislatore europeo, nell'introdurre il consenso fra le basi giuridiche idonee a derogare al divieto posto dal primo comma, ha ritenuto opportuno assistere la previsione con un'ulteriore garanzia, specificando il carattere necessariamente esplicito del consenso ivi disciplinato[343]. Ciò implica che la manifestazione di volontà richiesta per acconsentire all'adozione di una decisione unicamente automatizzata nei propri confronti, a differenza di quella richiesta dall'articolo 4(1) n.11 GDPR, non deve soltanto rivestire la forma di una dichiarazione o azione positiva ed inequivocabile, ma deve anche essere ulteriormente confermata. Ad esempio, l'interessato, per corroborare in modo più espresso la propria prestazione di consenso, potrebbe fornire al titolare una dichiarazione scritta, anche tramite *e-mail* o documentazione scansionata, ovvero avvalendosi della firma elettronica o compilando appositi moduli *online*[344].

Right for the Profiling Era, in J. BUS, M. CROMPTON, M. HILDEBRANDT, G. METAKIDES (a cura di), *Digital Enlightenment Yearbook 2012*, IOS Press, Amsterdam, 47.

[342] A. DE FRANCESCHI, *La circolazione dei dati tra privacy e contratto*, cit., 41. Cfr. L. EDWARDS e M. VEALE, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017, 39; M. ANNANY e K. CRAWFORD, Seeing Without knowing: limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 973-989; A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1192 ss; E. LUCCHINI GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 71 ss. Per riflessioni più approfondite in tema di trasparenza e comprensibilità delle informazioni (rectius spiegazioni) fornite al soggetto interessato, si veda *infra* nel prossimo paragrafo.

[343] Cfr. G. DE GREGORIO, R. TORINO, *Privacy, protezione dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 478 ss.

[344] Vale la pena ricordare che, ancora prima della verifica del carattere esplicito della manifestazione di consenso, questa dovrebbe comunque risultare positiva ed inequivocabile. In virtù del primo aspetto, è quindi invalido il consenso prestato con la semplice prosecuzione dell'utilizzo del servizio (e.g. scorrendo verso il basso o muovendosi fra le pagine di sito web). In virtù del secondo requisito, come peraltro già menzionato nel testo, non costituirebbe una univoca manifestazione di volontà la prestazione del consenso in occasione dell'accettazione delle condizioni del servizio, ovvero la prestazione del consenso cumulativa per più finalità diverse di trattamento. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 18; RAPPORTEUR JAN PHILIPP ALBRECHT, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free

Tale ulteriore adempimento, specialmente nelle more dell'implementazione di adeguati sistemi di *privacy by default*[345], attenuerebbe anche il rischio della trasformazione della prestazione del consenso in un c.d. "*tick-box exercise*"[346], tipico del contesto *online*, e conseguenza delle numerose e frequenti richieste di consenso che quotidianamente interferiscono con la fruizione dei servizi online da parte degli utenti[347].

Da ultimo, e strettamente legato al requisito della libertà, è poi il requisito della c.d. (non) condizionalità del consenso, sancito dall'articolo 7 co.4 GDPR in virtù del quale "[n]el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto"[348].

Nella misura in cui mira ad evitare che il consenso si trasformi in un corrispettivo obbligatorio per la prestazione del servizio, la verifica della condizionalità del consenso è strettamente interconnessa a quella della necessarietà del trattamento dei dati, ai fini dell'esecuzione del contratto: seconda e diversa base giuridica per derogare al divieto di cui all'articolo 22 co.1 GDPR. Ai sensi dell'articolo 22 co.2 lett. a GDPR, infatti, il primo

movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Comitato per le libertà civili, la giustizia e gli affari interni, 21 novembre 2013), 10.

[345] Cfr. 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, Giuffré, 2019, 486 ss; G. D'ACQUISTO e M. NALDI, *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*, Giappichelli Editore, Torino, 2017, 34 ss. Sull'attuazione dei principi di *privacy by design* e *by default* si veda anche F. BRAVO, *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 793 ss; F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, 271 ss ; F. SARTORE, Privacy-by-design, *l'introduzione del principio nel* corpus *del GDPR*, S.F. GIOVANNANGELI, *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 296 ss.

[346] In questi termini si è espresso Buttarelli. G. BUTTARELLI, Keynote speech on privacy, data protection and cyber security in the era of AI (*Telecommunications and Media Forum: Artificial Intelligence and the future Digital Single Market*, 24 April 2018), 4.

[347] Sull'invalidità del consenso prestato a seguito di richieste che interferiscono "inutilmente" con la fruizione del servizio, si veda GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 18.

[348] Sulla questione del "consenso forzato" per l'accesso a beni e servizi si veda anche V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, cit., 38 ss.

comma non si applica nel caso in cui la decisione "sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento"[349].

Ne consegue che, se il trattamento dei dati (non sensibili)[350] è necessario (*rectius* indispensabile) per dare esecuzione al contratto (o adottare misure precontrattuali), il titolare del trattamento potrà prescindere dal consenso del soggetto interessato. Da notare, tuttavia, che se il trattamento dei dati è sì "necessario", ma soltanto al fine di garantire la remuneratività del servizio offerto "gratuitamente" al cliente, ad esempio attraverso la trasmissione dei dati raccolti attraverso il tracciamento dell'attività dell'utente per finalità di *marketing* personalizzato, il titolare del trattamento non potrà avvalersi della base giuridica della necessità[351].

In senso contrario, si era espresso il Comitato per il mercato interno e la protezione dei consumatori che, in fase di consultazione, aveva proposto l'introduzione di uno specifico considerando in cui menzionare espressamente la possibilità di individuare nella revoca del consenso una idonea causa di scioglimento del contratto, in tutti i casi in cui l'offerta del servizio *online* fosse remunerata tramite l'accesso ai (e il trattamento dei) dati personali dei propri clienti[352]. In questo modo, sosteneva il *Rapporteur* Lara Comi,

[349] Cfr. T. GROTTO, M. CASADIO, *La certificazione dei consensi raccolti* online, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 356 ss.

[350] Nel caso in cui oggetto del trattamento sia dati sensibili, l'articolo 22 co.4 GDPR restringe l'operatività delle deroghe fissate dal secondo comma al divieto. In particolare, le decisioni unicamente automatizzate prese sulla scorta di una delle tre basi giuridiche fissate dall'articolo 22 co.2 non possono basarsi su categorie di dati sensibili, salvo che l'interessato abbia prestato il suo consenso esplicito (per finalità specifiche), ovvero "il trattamento [risulti] necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato". Cfr. M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 235 ss.

[351] Cfr. I. DESTRI e A.M. LOTTO, *La profilazione*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018, 141 ss; C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 680 ss.

[352] V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, 108 ss. Cfr. A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, Giuffrè editore, Milano, 2007, 241 ss.

si sarebbe innalzato il livello di consapevolezza degli utenti circa la natura "monetaria" assunta dai loro dati personali, assimilabili alle "monete con cui pagano per il servizio"[353].

Tale prospettiva, tuttavia, non recepita nella versione finale del regolamento, è stata recentemente disattesa anche dallo *European Data Protection Board* (EDPB), il quale ha puntualizzato che il *behavioural advertising* non può essere considerato un elemento essenziale del diverso servizio che serve a finanziare[354]. Ciò sarebbe confermato, da un lato, dal diritto dei soggetti interessati di potersi opporre, in ogni momento, al trattamento dei propri dati personali per finalità di *marketing* diretto (articolo 21 GDPR). Dall'altro, dalla considerazione per cui i soggetti interessati, pur potendo acconsentire al trattamento dei propri dati personali, non possono scambiare o cedere i propri diritti fondamentali, fra cui rientra il diritto alla protezione dei propri dati personali *ex* art. 8 Carta di Nizza[355]. Nell'ottica adottata dallo EDPB, quindi, i dati personali non sarebbero assimilabili ad una c.d. *tradeable commodity*[356], né tantomeno ad una nuova

[353] RAPPORTEUR LARA COMI, *Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), 28 gennaio 2013, 411ss. Cfr. G. MALGIERI, B. CUSTERS, Pricing Privacy, cit., 189 ss; F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cit., 12 ss; S.A. ELVY, Paying for privacy and the personal data economy, 117, *Columbia Law rev*., 6, 2017, 1369 ss.

[354] Cfr. G. NOTO LA DIEGA, *Data as Digital Assets. The Case of Targeted Advertising*, in M. BAKHOUM, B. CONDE GALLEGO, M.O. MACKENRODT, G. SURBLYTE-NAMAVICIENE (a cura di), *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach*?, MPI Studies on Intellectual Property and Competition Law, Vol. 28, Springer, Berlino, 2018, 445 ss.

[355] Sulla riconducibilità del dato personale ad attributo della personalità si veda meglio *supra* nel precedente capitolo. Cfr. G. AGRIFOGLIO, Risarcimento e quantificazione del danno da lesione della *privacy*: dal danno alla persona al danno alla personalità, 4, *Europa e Diritto Privato*, 2017, 1265 ss. Cfr. E. TOSI, Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE, *Danno e responsabilità*, 4, 2020, 433 ss; ID., La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR) (prima parte)., *Studium Iuris*, 7-8, 2020, 840 ss; ID., La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR)(seconda parte), *Studium Iuris*, 9, 2020, 1032 ss; ID., Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo, *Contratto e impresa*, 3, 2020, 1115 ss.

[356] Per una riflessione sui dati come "merci" vedi anche C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 676 ss. Sul punto si veda anche G. ALPA, *La "proprietà" dei dati personali*, cit., 18 ss. In senso contrario J.M. VICTOR, The Eu General Data Protection regulation: Toward a Property Regime for Protecting Data Privacy, 513 ss. Cfr. J. CIANI, Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, cit., *passim*; P. SCHWARTZ, Property, Privacy and Personal Data, cit., 2055, *passim*.

forma di valore monetario, poiché suscettibili di utilizzo non rivale, e privi della capacità di fungere da unità di conto e riserva di valore[357].

Di conseguenza, nei casi in cui il trattamento risulti necessario per sole finalità di miglioramento e/o finanziamento del servizio offerto, il titolare dovrà dimostrare di non aver condizionato la prestazione del servizio al consenso dell'interessato-cliente. A tal proposito, il Gruppo di lavoro articolo 29 ha specificato che tale onere probatorio non potrebbe essere assolto con l'allegazione della possibilità, per l'interessato, di avvalersi di un servizio analogo offerto da altro operatore, per la fruizione del quale non viene richiesto il trattamento dei dati per finalità di *marketing*[358].

Al contrario, il titolare del trattamento potrebbe superare la presunzione di condizionalità del consenso garantendo agli interessati la possibilità di revocarlo, in ogni momento, senza subire alcun pregiudizio (inclusa una ridotta operatività del servizio). L'articolo 7 co. 3 GDPR, peraltro, codificando una posizione già avanzata dal Gruppo di lavoro articolo 29[359], si è premurato di precisare che la revoca del consenso deve poter avvenire con la stessa facilità con cui è stato prestato[360]. Ciò significa, ad esempio, che per poterne escludere la condizionalità, il consenso dovrebbe essere revocabile tramite la medesima interfaccia su cui è stato prestato, senza imporre alcun passaggio ulteriore[361].

Poco prima che le linee guida del 2019 fin qui analizzate venissero poste in pubblica consultazione, tuttavia, la Corte di Cassazione era giunta a conclusioni opposte. In particolare, con la sentenza n. 17278/2018, e con riferimento al previgente articolo 23

[357] EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, adottate il 9 aprile 2019 (versione per la consultazione pubblica), §§ 48-52. Cfr. A. DE FRANCESCHI, Il "pagamento" mediante dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1384 ss; V. RICCIUTO, La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, 4, *Diritto dell'Informazione e dell'Informatica*, 2018, 689 ss.

[358] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 10 e 22. In questo stesso senso si esprime anche il considerando 42, per cui nel caso di "trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento".

[359] Cfr. Così GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 15/2011 on the definition of consent*, adottato il 13 luglio 2011 (WP187), 32 ss.

[360] Cfr. G. RESTA, Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali, cit., 299, *passim*.

[361] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 28 novembre 2017 (come modificate e adottate da ultimo il 10 aprile 2018) (WP 259 rev.01), 24.

Codice della *Privacy*, aveva ritenuto che, pur configurando un consenso "rafforzato", la disciplina in materia di protezione dei dati personali consentisse "al gestore di un sito Internet, il quale somministri un servizio fungibile, cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di *newsletter* su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, sempre che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta altresì la necessità, almeno, dell'indicazione dei settori merceologici o dei servizi cui i messaggi pubblicitari saranno riferiti"[362].

Al di là dell'ipotesi del *marketing*, qualora il titolare del trattamento non possa avvalersi del (o non sia in grado di dimostrare il)[363] consenso esplicito, libero, specifico,

[362] In punto di fatto, la pronuncia prende le mosse dall'appello proposto dal Garante Privacy (e accolto dalla Suprema Corte) avverso la sentenza con cui il Tribunale di Arezzo aveva ritenuto fondata l'opposizione di un prestatore di un servizio di *newsletter* su tematiche legate alla finanza, al fisco, al diritto e al lavoro ad un provvedimento con cui il Garante aveva dichiarato illecito il trattamento posto in essere dalla società. In particolare, l'Autorità garante aveva ritenuto che il consenso raccolto dal titolare del trattamento non fosse libero e specifico, perché non conforme alle linee guida da esso elaborate e con cui veniva fornita la corretta interpretazione del dato normativo (*i.e.* l'articolo 23 Codice *Privacy*). Il Tribunale, dal canto suo, aveva invece ritenuto che tali indicazioni del Garante operassero una inammissibile integrazione del dato normativo, posto che "la norma non individua un obbligo *tout court* per il gestore del portale di offrire comunque le proprie prestazioni, a prescindere dal consenso al trattamento dei dati personali da parte dell'utente". Investita della questione, la Cassazione ha accolto il ricorso del Garante, ritenendo che il consenso, nel caso di specie, non fosse qualificabile come libero e specifico. Ciò in quanto l'iscrizione alla *newsletter* veniva condizionata alla prestazione di un consenso con cui si autorizzava, contestualmente, tanto l'utilizzo dei dati per l'invio delle comunicazioni richieste quanto di comunicazioni promozionali, senza poter scindere le due manifestazioni di volontà e senza che, peraltro, fosse specificata la natura e l'oggetto di queste ultime. Ciononostante, la Corte di Cassazione ha puntualizzato che tale conclusione non possa essere generalizzata nella misura in cui " il condizionamento non possa sempre e comunque essere dato per scontato e debba invece essere tanto più ritenuto sussistente, quanto più la prestazione offerta dal gestore del sito Internet sia ad un tempo infungibile ed irrinunciabile per l'interessato, il che non può certo dirsi accada nell'ipotesi di offerta di un generico servizio informativo del tipo di quello in discorso, giacché all'evidenza si tratta di informazioni agevolmente acquisibili per altra via, eventualmente attraverso siti a pagamento, se non attraverso il ricorso all'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio. […] Nulla, infatti, impedisce al gestore del sito – beninteso, si ripete, in un caso come quello in questione, concernente un servizio né infungibile, né irrinunciabile -, di negare il servizio offerto a chi non si presti a ricevere messaggi promozionali, mentre ciò che gli è interdetto è utilizzare i dati personali per somministrare o far somministrare informazioni pubblicitarie a colui che non abbia effettivamente manifestato la volontà di riceverli. Insomma, l'ordinamento non vieta lo scambio di dati personali, me esige tuttavia che tale scambio sia frutto di un consenso pieno ed in nessun modo coartato". Per un commento alla sentenza v. S. THOBANI, Protezione dei dati personali - operazioni di *tying* e libertà del consenso, 3, *Giur. It*., 2019, 530 ss; F. BRAVO, Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto, 1, *Contratto e impres*a, 2019, 34 ss; F. ZANOVELLO, Consenso libero e specifico alle *e-mail* promozionali, 12, NGCC, 2018, 1175 s; G. ALPA, *La "proprietà" dei dati personali*, cit., 22-23.

[363] Sul concetto di prova liberatoria in materia di trattamento dei dati personali si veda anche M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 1060 ss.

informato e non condizionato, quale base giuridica *ex* art. 22 GDPR, la decisione unicamente automatizzata eventualmente presa nei confronti dell'interessato non sarà illegittima se necessaria all'esecuzione di un contratto (o di misure precontrattuali), ovvero se autorizzata dalla legge.

Con riferimento alla prima, l'esigenza di salvaguardare l'effettività del divieto fissato dall'articolo 22 co.1 GDPR, già compromessa dalle numerose condizioni di operatività descritte nel precedente paragrafo[364], rende opportuno adottare un'interpretazione rigorosa della nozione di necessità contrattuale (e precontrattuale)[365].

In questo senso, ad esempio, non possono essere considerate necessarie all'esecuzione del contratto tutte quelle azioni che ineriscono alla fase patologica dello stesso. Il titolare del trattamento non potrebbe quindi avvalersi di questa base giuridica per adottare decisioni concernenti, fra gli altri, l'esperimento di un'azione giurisdizionale o, più genericamente, misure di recupero crediti. Come osservato dal Gruppo di lavoro articolo 29, in questi casi il titolare del trattamento potrebbe astrattamente avvalersi della diversa base giuridica dell'interesse legittimo per trattare i dati personali dell'interessato[366]. Ciononostante, è opportuno puntualizzare che tale base giuridica, seppure disciplinata in via generale dall'articolo 6 co.1 lett. f GDPR, non è parimenti richiamata dall'articolo 22 GDPR. Di conseguenza, il titolare del trattamento non potrebbe mai avvalersi di processi decisionali unicamente automatizzati per adottare determinazioni concernenti la fase patologica del rapporto contrattuale in essere col soggetto interessato.

In secondo luogo, la circostanza per cui l'automazione dei processi decisionali potrebbe essere utile a massimizzare la correttezza, l'efficienza e la precisione delle determinazioni adottate, non è sufficiente a renderla necessaria *ex* art. 22 GDPR[367]. Ciò

[364] Cfr. E. PELLECCHIA, *Privacy, decisioni automatizzate e algoritmi*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 429 ss.

[365] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014, (844/14/IT), 21.

[366] Cfr. C. D'AGATA, Il legittimo interesse del titolare o di un terzo nel quadro dei diversi presupposti di legittimità del trattamento, in R. PANETTA (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018, Milano, Giuffré, 2019, 82 ss.

[367] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 14.

in quanto, come opportunamente precisato da Giovanni Buttarelli "[*n]ot everything that "might prove to be useful" for a certain purpose is "desirable or can be considered as a necessary measure in a democratic society*"[368].

Allo stesso modo, non è valido indice del carattere necessario del trattamento automatizzato, il fatto che ne sia stata fatta espressa menzione nel testo del contratto sottoscritto dal soggetto interessato[369]. Al contrario, l'interprete è chiamato a condurre un quadruplice test di necessità volto a vagliare, in concreto, la necessarietà contrattuale di ogni singola componente del trattamento automatizzato a fini decisionali.

Più specificamente, i primi due passaggi del test di necessità vengono tradizionalmente individuati nella ricostruzione delle caratteristiche operative del trattamento dei dati. Ciò al fine di valutare se, considerate le categorie di dati trattati, le modalità di raccolta e analisi degli stessi, l'identità del titolare, nonché la durata del trattamento, quest'ultimo possa concretamente determinare una limitazione del diritto alla protezione dei dati personali dell'interessato-controparte contrattuale.

Nel caso dei processi decisionali automatizzati, tuttavia, tale passaggio viene per ovvie ragioni assorbito dall'espresso divieto sancito dall'articolo 22 GDPR, rispetto al quale la necessità contrattuale si pone *ab origine* come deroga.

Mantengono invece la loro rilevanza il terzo e il quarto passaggio del test di necessità. In particolare, dimostrata l'esistenza di un contratto valido, se ne dovranno individuare l'oggetto (i.e. la natura del servizio offerto) e la *ratio* (i.e. l'interesse generale perseguito). Alla luce di quanto così emerso, si procederà poi a ricostruire le aspettative degli utenti riguardo alle possibili finalità e modalità del trattamento dei dati forniti in sede di conclusione del contratto. A tal fine, saranno tenute in considerazione anche le informazioni diffuse dal titolare del trattamento a livello pubblicitario.

---

[368] GIOVANNI BUTTARELLI, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, EDPB, 11 aprile 2017, 18. Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services*, adottate il 9 novembre 2004, (WP 99).

[369] EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, adottate il 9 aprile 2019 (versione per la consultazione pubblica), § 27; GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014, (844/14/IT), 20.

Fissato così il contesto di riferimento, sarà possibile procedere con i due passaggi della verifica rimasti pertinenti, in virtù dei quali, la decisione unicamente automatizzata potrà essere considerata necessaria se: (i) appare compatibile e coerente alla natura del servizio offerto; e (ii) risulta effettivamente impossibile procedere alla conclusione o l'esecuzione del contratto in sua mancanza[370].

Tali condizioni, tuttavia, non sarebbero soddisfatte ove il trattamento fosse finalizzato all'assunzione di decisioni unicamente automatizzate concernenti il grado di rischio dell'interessato, tanto a fini assicurativi, quando creditizi[371]. Ciò in quanto, sebbene l'art. 22 co.2 lett. a GDPR non condizioni più la base giuridica della necessità del processo decisionale automatizzato alla previa formulazione (e successivo accoglimento) di una richiesta sul punto da parte del soggetto interessato[372], molte delle informazioni suscettibili di trattamento nel contesto *Big Data* non sono necessarie alla conclusione del contratto, quanto piuttosto ad una più efficiente gestione del rischio allo stesso connesso. Dovrebbero perciò applicarsi le stesse considerazioni svolte con riferimento all'inadeguatezza della base giuridica della necessità per l'ipotesi del *marketing* personalizzato.

Potrebbe allora venire in soccorso la terza e ultima base giuridica disciplinata dall'articolo 22 co. 2 lett. b GDPR per legittimare l'adozione di decisioni unicamente automatizzate, ove queste ultime siano autorizzate "dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato".

Tale fattispecie, prevista anche dall'articolo 15 co.2 lett. b Dir. 1995/46/CE, ricorre ogniqualvolta il titolare del trattamento possa invocare, a giustificazione della decisione assunta, un obbligo imposto dalla legge dello Stato, dell'Unione Europea, ovvero dell'ordinamento internazionale, a condizione che risulti sufficientemente chiaro

[370] GIOVANNI BUTTARELLI, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, EDPB, 11 aprile 2017, 10.

[371] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014, (844/14/IT), 22.

[372] In particolare, l'articolo 15 Dir. 1995/46/CE stabiliva che una persona avrebbe potuto essere sottoposta ad una decisione fondata esclusivamente su un trattamento automatizzato qualora quest'ultima fosse "presa nel contesto della conclusione o dell'esecuzione di un contratto, a condizione che la domanda relativa alla conclusione o all'esecuzione del contratto, presentata dalla persona interessata [fosse] stata accolta, oppure che misure adeguate, fra le quali la possibilità di far valere il proprio punto di vista [garantissero] la salvaguardia del suo interesse legittimo".

e specifico. Ne discende che l'operatività di tale base giudica è neutralizzata in tutti i casi in cui il titolare del trattamento mantiene la possibilità di scegliere se adempiere o meno all'obbligo, si spinge oltre quanto espressamente imposto, ovvero dispone di un ampio margine di discrezionalità circa le modalità di adempimento[373].

Tale ultima ipotesi ricorre, ad esempio, ogniqualvolta la legge si limiti a fornire orientamenti politici generali, come avviene in ambito bancario in punto di valutazione del merito creditizio della clientela e conseguente decisione circa la concessione o meno di finanziamenti. Sul punto, infatti, è ormai pacifico come, da un lato, non esista in capo agli intermediari un obbligo di erogare il credito[374] e, dall'altro, l'apprezzamento del merito creditizio costituisca espressione del rischio imprenditoriale degli intermediari, ed integri un'attività tecnica che questi ultimi effettuano "nel rispetto delle norme prudenziali che riconoscono, pur entro specifici canoni tecnici, ampia discrezionalità legata alla natura imprenditoriale dell'attività di erogazione del credito, sulla base di conoscenze tecnico scientifiche di non univoca valutazione"[375].

---

[373] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, adottato il 9 aprile 2014, (844/14/IT), 23.

[374] In questo senso si esprime il costante orientamento dell'Arbitro Bancario Finanziario della Banca d'Italia (ABF), per il quale "non può considerarsi esistente, alla luce dell'attuale disciplina generale della materia, un diritto del cliente alla concessione del credito, data l'indubbia autonomia decisionale da riconoscersi all'intermediario in ordine alla relativa erogazione sulla base di proprie valutazioni". Invero, un obbligo generale di far credito è certamente estraneo allo statuto delle imprese bancarie, la cui attività deve ispirarsi ai principi di una "sana e prudente gestione" e deve essere esercitata avendo riguardo "alla stabilità complessiva, all'efficienza e alla competitività del sistema finanziario" (arg. ex art. 5 d.lgs. 1° settembre 1993, n. 385) (Cfr., in tal senso, Collegio di Milano, decisione n. 904 del 2.02.2017). Né tanto meno l'ABF può sostituirsi all'intermediario, imponendogli la concessione di un finanziamento, in quanto la valutazione del merito creditizio rimane prerogativa dell'istituto erogante. In altri termini, la scelta circa l'accettazione di una richiesta di finanziamento rientra senz'altro nell'autonomia gestionale della banca". Così, da ultimo, Collegio di Roma, Decisione N. 1339 del 17 gennaio 2019. In senso analogo si esprime anche la giurisprudenza di merito, *ex multis* Trib. Roma sez. VIII, Sent. 3 giugno 2017, n. 11238, che richiamando le decisioni ABF del 12 febbraio 2013 n. 819 e del 14 agosto 2014 n. 5222, ha stabilito come non possa ritenersi sussistente alcuna obbligazione di contrarre in capo alle banche, essendo libere di valutare il merito creditizio del richiedente, seppure nel rispetto degli obblighi di correttezza e informazione che discendono dal principio generale della buona fede. Cfr. G. MATTARELLA, Big Data e accesso al credito degli immigrati: discriminazioni algoritmiche e tutela del consumatore, *Giurisprudenza Commerciale*, 4, 2020, 696 ss.

[375] Tale valutazione risulta quindi insindacabile, salvo risulti evidente la sussistenza di uno sviamento logico, di un errore di fatto, ovvero la motivazione appaia manifestamente contraddittoria. Cfr. Arbitro Bancario Finanziario, Collegio di Bologna, Decisione n. 4293 del 12 febbraio 2019. Ancora oltre si è spinta la Corte di Giustizia dell'Unione Europea, che investita di una questione pregiudiziale concernente la corretta interpretazione dell'articolo 5, paragrafo 6 e dell''articolo 8, paragrafo 1, della direttiva 2008/48 ha stabilito che tali disposizioni "non ostano a una normativa nazionale, come quella di cui trattasi nel procedimento principale, la quale impone al creditore di astenersi dal concludere il contratto di credito qualora non possa ragionevolmente ritenere, al termine della verifica del merito creditizio del consumatore, che quest'ultimo sarà in grado di rispettare gli obblighi derivanti dal contratto di cui trattasi". Sentenza della Corte di Giustizia (Prima Sezione) del 6 giugno 2019 (domanda di pronuncia pregiudiziale

Alla luce delle considerazioni sin qui condotte, si può quindi concludere che le banche e gli altri intermediari finanziari, così come le assicurazioni, non potrebbero in alcun caso adottare decisioni unicamente automatizzate *ex* art. 22 GDPR. Ciò in quanto, in primo luogo, il fisiologico squilibrio di potere tra le parti neutralizza il carattere libero del consenso, rendendo così tale base giuridica inidonea allo scopo. In secondo luogo, l'amplia pletora di dati non strutturati (e non finanziari) resi disponibili dall'avvento dei *Big Data*, per quanto precisa possa rendere la ricostruzione del livello di rischiosità del cliente, è difficilmente configurabile come necessaria a fini contrattuali. Da ultimo, il carattere ontologicamente insindacabile e discrezionale della valutazione del merito credito, rende gli obblighi legislativi in materia di diligenza e trasparenza troppo generici per qualificarsi quale base giuridica ai sensi dell'articolo 22 co.2 lett. b GDPR.

Ciononostante, le molteplici condizioni di applicazione del divieto fissate dal primo comma dell'articolo 22 GDPR, associate alla potenziale ampiezza delle deroghe ammesse dal secondo comma, nonché ai molteplici dubbi interpretativi sollevati da entrambi i capoversi, rendono di tutta evidenza come la reale tutela apprestata dalla disposizione, risieda nelle "misure appropriate" di cui al terzo comma. In particolare, il legislatore europeo del 2016 ha ritenuto opportuno precisare che, qualora l'interessato presti il proprio consenso esplicito all'adozione di una decisione unicamente automatizzata nei suoi confronti, ovvero quest'ultima si renda contrattualmente necessaria, il titolare del trattamento è comunque tenuto a predisporre "misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato", fra cui "almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione".

Per questa ragione, il proseguo del capitolo si ripropone di riflettere, in via generale, sul grado di effettività della tutela apprestata da tali strumenti legislativi di contenimento del rischio e, più nello specifico, sulla configurabilità di un diritto di spiegazione.

proposta dalla *Justice de Paix du canton de Visé* — Belgio) — *Michel Schyns/Belfius Banque SA* (Causa C-58/18) (2019/C 263/14).

2.4. Le informazioni significative sulla logica: una spiegazione?

Come accennato, nel caso in cui la sfera giuridica di un soggetto interessato sia intaccata da una decisione basata unicamente sul trattamento automatizzato dei suoi dati personali, perché vi ha acconsentito ovvero perché contrattualmente necessaria, il legislatore europeo ha posto in capo al titolare del trattamento l'obbligo di adottare "misure appropriate" per tutelare i diritti, le libertà e i legittimi interessi dell'interessato[376]. Tali misure dovrebbero comprendere "almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione"[377]. In senso analogo, il considerando 71 GDPR puntualizza che le suddette garanzie "dovrebbero comprendere la *specifica* informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una *spiegazione della decisione* conseguita *dopo* tale valutazione e di contestare la decisione"[378].

A partire da tale disposto normativo, la dottrina si è innanzitutto interrogata circa la configurabilità di un vero e proprio diritto ad una spiegazione della specifica decisione automatizzata.

Il dibattito prese le mosse da una riflessione inizialmente avanzata da Bryce Goodman e Seth Flaxman[379], due studiosi di Oxford convinti che l'articolo 22 GDPR fosse potenzialmente in grado di proibire l'utilizzo di un'ampia pletora di algoritmi di profilazione attualmente sfruttati a fini di *marketing* diretto, valutazioni finanziarie, assicurative, per l'implementazione di "suggerimenti" su *social networks*, e molto altro. In particolare, nelle parole degli Autori "[*t*]*he GDPR's policy on the right of citizens to*

[376] Articolo 22 paragrafo 3 GDPR. Cfr. C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 718-719; A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 242 ss; E. PELINO, *I diritti dell'interessato*, IN E. PELINO, L. BOLOGNINI, C. BISTOLFI, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffré, Milano, 2016, 268-269.

[377] *Ibid*.

[378] Corsivo aggiunto. Sulla portata del dovere informativo ivi disciplinato cfr. A. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 443 ss. Cfr. B. CASEY, A. FARHANGI, R. VOGL, Rethinking Explainable Machines: the GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise, 34, *Berkeley Tech. L.J.*, 2019, 143ss.

[379] B. GOODMAN e S.FLAXMAN, European Union regulations on algorithmic decision-making and a "right to explanation", 38, *AI Magazine*, 3, 2017, presentato per la prima volta nel 2016 al ICML Workshop relative al tema della Human Interpretability in Machine Learning (WHI 2016), New York, NY.

receive an explanation for algorithmic decisions highlights the pressing importance of human interpretability in algorithm design"[380].

Sebbene le argomentazioni a supporto di tale intuizione non vadano molto oltre la rappresentazione dell'esigenza di prevenire e contrastare la discriminazione algoritmica[381] attraverso una più sensibile ponderazione del *trade-off* tra precisione predittiva e comprensibilità del processo decisionale automatizzato, è evidente che gli autori individuano il fondamento normativo del diritto ad una spiegazione non soltanto nelle "misure adeguate" di cui all'articolo 22 GDPR, ma anche e soprattutto nelle concrete modalità attuative dei doveri informativi di cui agli articoli 13, 14 e 15 GDPR[382].

Ai sensi del combinato disposto degli articoli 13 para 2 lett. f e 14 para 2 lett. g GDPR, infatti, a prescindere dalla circostanza per cui i dati personali trattati a fini decisionali siano raccolti presso terzi o presso l'interessato, il titolare del trattamento deve fornire a quest'ultimo informazioni relative all'"esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, *informazioni significative sulla logica utilizzata*, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"[383]. La medesima formulazione è poi utilizzata dall'articolo 15 para 1 lett. h GDPR che, tuttavia, come si vedrà meglio nel proseguo del paragrafo, sembrerebbe estendere tali doveri informativi anche nella fase successiva all'avvio del trattamento e all'assunzione della decisione automatizzata.

La posizione inizialmente avanzata da Goodman e Flaxman, tuttavia, non ha mancato di suscitare critiche. Furono proprio altri studiosi di Oxford, Wachter, Mittelstadt

[380] IVI, 1.

[381] Per riflessioni più approfondite sui rischi posti dalla c.d. "*behavioral discrimination*" basata sui *Big Data* si veda A. EZRACHI e M. STUCKE, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Boston, Harvard University Press, 2016, 86-87; K. CRAWFORD e J. SCHULZ, *Big Data* and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55, *Boston College Law Rev*, 93, 2014, 119; D. KEATS CITRON e F. PASQUALE, The Scored Society: Due Process for Automated Predictions, 89, *Washington Law Review*, 2014, 1, 10ss; TOON CALDERS e INDRĖ ŽLIOBAITĖ, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society*. *Data Mining and Profiling in Large Databases*, Springer, New York, 2013, 49-53; F. ZUIDERVEEN BORGESIUS, *Discrimination, artificial intelligence, and algorithmic decision-making* (Consiglio d'Europa, Strasburgo 2018), 10 ss; P. HACKER, Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law, 55, *Common Market Law Review*, 4, 2018, 1143ss.

[382] B. GOODMAN e S. FLAXMAN, European Union regulations on algorithmic decision-making and a "right to explanation", 38, *AI Magazine*, 3, 2017, 6.

[383] Corsivo aggiunto.

e Floridi, i primi a formulare una lettura alternativa del dato normativo fin qui analizzato, sostenendo che il GDPR nella sua attuale formulazione non riconoscerebbe il diritto ad una spiegazione *ex post* delle specifiche decisioni assunte, ma un più limitato diritto ad essere *ex ante* informati sulle caratteristiche generali di funzionamento del sistema di IA utilizzato[384].

Il primo argomento a supporto di tale conclusione è di matrice letterale: il diritto ad una "spiegazione" viene espressamente menzionato esclusivamente a livello dei considerando, in particolare nel considerando 71 GDPR, al quale, notano gli Autori, non può che attribuirsi un valore meramente interpretativo e non portatore di autonomi precetti normativi[385].

I lavori preparatori all'adozione del GDPR, peraltro, contribuirebbero a suffragare ulteriormente tale posizione, poiché confermerebbero il carattere deliberato e consapevole della scelta legislativa compiuta. Si fa notare, infatti, che sebbene il Parlamento europeo avesse proposto di emendare la versione originaria dell'attuale articolo 22 GDPR sancendo espressamente che "la profilazione […] non deve essere basata unicamente o prevalentemente sul trattamento automatizzato e deve includere una valutazione umana, *inclusa una spiegazione della decisione raggiunta* dopo tale valutazione"[386], la versione finale del Regolamento ha invece fatto propria la formulazione proposta dal Consiglio europeo non soltanto per il linguaggio utilizzato

[384] SANDRA WACHTER, BRENT MITTELSTADT e LUCIANO FLORIDI, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7, *International Data Privacy Law*, 2, 2017, 76, 77.

[385] Gli Autori sottolineano, peraltro, come, data la somiglianza che il linguaggio utilizzato nel considerando 71 presenta con quello dell'articolo 22 GDPR, ove il legislatore avesse voluto riconoscere un siffatto diritto, avrebbe incluso il "diritto ad ottenere una spiegazione" nel paragrafo 3 dell'articolo e non si sarebbe limitato a menzionarlo nel solo considerando. IVI, 80-81.

[386] Corsivo aggiunto. Così la formulazione in lingua originale dell'allora articolo 20 della proposta di regolamento "*Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment. The suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 shall include the right to obtain human assessment and an explanation of the decision reached after such assessment*". RAPPORTEUR JAN PHILIPP ALBRECHT, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Civil Liberties, Justice and Home Affairs, 21 novembre 2013), 94.

nell'articolo, ma anche per la scelta di confinare la menzione di una spiegazione al solo livello dei considerando[387].

Tale ricostruzione, tuttavia, per quanto testualmente fedele, minimizza in modo forse eccessivo il ruolo dei considerando che, per quanto meramente interpretativo, trova comunque ragion d'esistere nella misura in cui chiarisce la portata dell'espressione "misure adeguate" utilizzata dal legislatore nell'articolo 22 para 3 GDPR[388]. Che la dimensione teleologica abbia un ruolo preponderante nell'esegesi della normativa eurounitaria, più di quanto una presunta *intentio legis* storicamente ricostruita dai lavori preparatori possa far pensare, è confermato poi dall'analogo dibattito sorto circa il significato da attribuire al carattere "unicamente" automatizzato delle decisioni *ex* art. 22 GDPR. Come già menzionato[389], infatti, seppure la proposta del Parlamento europeo di considerare decisioni basate unicamente "o *prevalentemente*" sul trattamento automatizzato dei dati personali non sia poi confluita nella versione finale del Regolamento, il Gruppo di Lavoro di cui all'Articolo 29 non ha mancato di puntualizzare che "il titolare del trattamento non può eludere le disposizioni dell'articolo 22 creando coinvolgimenti umani fittizi. […] [Poiché] [p]er aversi un coinvolgimento umano, il titolare del trattamento deve garantire che qualsiasi controllo della decisione sia significativo e non costituisca un semplice gesto simbolico"[390]. Se ne deduce, quindi, che gli obiettivi sottesi la fallita puntualizzazione linguistica rimangono parte integrante degli

[387] COMMISSIONE EUROPEA, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (*General Data Protection Regulation*), Bruxelles, 2012, COM(2012) 11 fin.

[388] Sul valore interpretativo dei considerando, con specifico riguardo alla configurabilità di un diritto ad una spiegazione, si veda G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243, 254-255, spec. nt. 85, ove viene richiamata la copiosa giurisprudenza della Corte di Giustizia sul punto. In particolare, gli Autori notano come "*it has been argued that recitals are not legally binding. Therefore, data controllers do not have a real duty to explanation according to Article 22(3) and Recital 71 GDPR. However, although it is undoubted that recitals are interpretative tools, they sometimes also perform a supplementary normative role. Even the European Commission confirms this supplementary normative nature of recitals. Recitals can help explain the purpose and intent behind a normative instrument.* […] *In the specific case at stake, Recital 71 does not derogate from Article 22, neither does it amend it in a manner contrary to its wording. It only helps clarifying which 'safeguards' should be employed by data controllers who perform automated decision-making in cases of Article 22(2) (decisions for the performance of a contract or where the subject has given the consent to decision-making processing). In its illustrative nature, Recital 71 can be properly considered a supplementary normative tool*."

[389] Si veda meglio *supra* § 2.2.1.

[390] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 23. Cfr. UK INFORMATION COMMISSIONER'S OFFICE (ICO), *Feedback request- profiling and automated decision-making*, 2017, 19.

obiettivi perseguiti dalla disposizione, e possono essere raggiunti attraverso un'interpretazione teleologica della norma, alla quale contribuiscono anche i considerando.

Analogo scetticismo viene poi manifestato dagli Autori rispetto alla possibilità di fondare il riconoscimento di un diritto ad una spiegazione nei doveri di notifica di cui ai menzionati articoli 13 para 2 lett. f e 14 para 2 lett. g GDPR. Ciò in quanto, si sottolinea, tali disposizioni non farebbero alcun riferimento al caso in cui all'interessato sia attribuito il solo diritto di contestare la decisione automatizzata, non rifiutabile perché fondata su una legittima base giuridica *ex* art. 22 para 2 GDPR. Ne conseguirebbe che, se anche dal combinato disposto degli articoli 13 e 14 GDPR fosse configurabile un qualche diritto ad una spiegazione, poiché gli stessi disciplinano doveri di notifica che devono essere assolti anteriormente all'effettivo inizio del trattamento e, conseguentemente, prima che la specifica decisione sia concretamente adottata, un eventuale diritto ad una spiegazione potrebbe esclusivamente consistere in una descrizione *ex ante* delle generiche caratteristiche di funzionamento del sistema di *machine learning* utilizzato. Di qui, la conclusione per cui sarebbe giuridicamente e tecnologicamente impossibile offrire una descrizione della specifica decisione adottata nel caso di specie nei confronti del singolo interessato[391].

A tal riguardo, sebbene sia innegabile che nel Regolamento manchi un collegamento testuale tra l'obbligo di adottare "misure appropriate" di cui all'articolo 22 para 3 GDPR (così come specificate in termini di "spiegazione della decisione" nel considerando 71) e il dovere di fornire "informazioni significative sulla logica utilizzata" di cui agli articoli 13 e 14 GDPR, è altrettanto evidente come la fattispecie presa in considerazione dalle disposizioni sia complessivamente la medesima. Ciò emerge chiaramente nella parte in cui il legislatore eurounitario ha tenuto a precisare che i doveri informativi *ex* artt. 13 e 14 GDPR operano *almeno* nel caso in cui l'interessato ha il diritto di non essere sottoposto alla decisione automatizzata, rimettendo tanto al legislatore nazionale quanto al titolare del trattamento stesso la facoltà di estenderne la portata. Peraltro, ove anche la decisione non sia rifiutabile dall'interessato, perché preceduta dalla

[391] A supporto di tale soluzione ermeneutica, gli Autori richiamano ancora una volta il dato testuale della norma, la quale, utilizzando espressioni quali "conseguenze *previste*", lascerebbe trapelare la prospettiva *pro futuro* adottata dal legislatore. SANDRA WACHTER, BRENT MITTELSTADT e LUCIANO FLORIDI, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7, *International Data Privacy Law*, 2, 2017, 76, 82-83.

prestazione del suo consenso, ovvero perché contrattualmente necessaria, il titolare del trattamento non è esente da obblighi informativi, ma anzi deve garantire *almeno* "il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione"[392].

Per di più si deve ricordare che, sebbene in quest'ultimo caso il GDPR non ponga in capo al titolare lo specifico obbligo di fornire all'interessato informazioni significative sulla logica utilizzata, il primo, ai sensi dell'articolo 12 GDPR, è comunque tenuto ad "agevol[are] l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22", e quindi anche il diritto di formarsi (per poi esprimere) un'opinione ed eventualmente contestare la decisione basata unicamente sul trattamento automatizzato dei propri dati ai sensi del terzo paragrafo dell'articolo 22 GDPR[393]. A tal fine, quindi, a prescindere dallo specifico linguaggio utilizzato dal legislatore, è evidente che in ogni ipotesi disciplinata dall'articolo 22 GDPR un qualche margine di *disclosure* della logica seguita dall'algoritmo è comunque richiesta.

Che poi questa *disclosure* possa riguardare soltanto la generica descrizione del funzionamento astratto del sistema di *machine learning* utilizzato, come sostenuto dagli Autori, è altrettanto discutibile. Se è vero che gli articoli 13 e 14 GDPR, nel disciplinare oneri informativi che devono essere assolti anteriormente all'inizio del trattamento,

[392] Tali tutele, tra l'altro, secondo quanto precisato dal considerando 71, dovrebbero applicarsi "in ogni caso" in cui venga adottata una decisione unicamente automatizzata, a prescindere dalla base giuridica che l'ha resa legittima. Da notare, inoltre, che in quest'ottica la lettura precedentemente avanzata per cui l'articolo 22 paragrafo 1 GDPR fisserebbe un divieto generale di adozione di decisioni interamente automatizzate, derogabile solo ove ricorra una delle eccezioni di cui al secondo paragrafo, sembrerebbe vacillare. Alla luce di una tale ricostruzione dei rimedi e delle garanzie offerte dal legislatore eurounitario, infatti, sembrerebbe che in realtà il primo paragrafo fissi un mero diritto di opposizione in capo al soggetto interessato che, conosciuta la decisione basata unicamente sul trattamento automatizzato, e in assenza di una delle basi giuridiche fissate dal secondo paragrafo, sarebbe messo nella condizione di poter meglio ponderare l'opportunità di rigettare la determinazione automatizzata sfruttando le informazioni "significative" sulla logica e sulle conseguenze dello stesso fornitegli dal titolare del trattamento. Nel caso in cui la decisione automatizzata fosse assunta sulla scorta di uno dei fondamenti di legittimità di cui all'articolo 22 paragrafo 2 lett. a (necessità contrattuale) e lett. c (consenso esplicito) GDPR, invece, il Regolamento sembrerebbe compensare l'assenza della possibilità di rigettare *tout court* la decisione, con il più blando diritto di ottenere l'intervento umano, al fine di esprimere la propria opinione e contestare (ma non rifiutare) la decisione. Cfr. A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 242.

[393] Sul carattere strumentale dei doveri informativi si veda F. PIRAINO, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, cit., 395; nonché F. CALISAI, *I diritti dell'interessato*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 336. Nelle parole di quest'ultimo, infatti, "Gli obblighi informativi sono senza dubbio da ritenersi funzionali all'esercizio dei diritti dell'interessato. Senza un'adeguata e trasparente circolazione e veicolazione delle informazioni sarebbe infatti precluso all'interessato stesso l'esercizio delle facoltà attribuitegli, che comprendono, come osservato, anche poteri di controllo e indirizzo".

presuppongano l'assunzione di una prospettiva ipotetica e la divulgazione di informazioni astratte relative al funzionamento del sistema, non è altrettanto vero che questo implichi l'inesistenza di un diritto ad una spiegazione *ex post* della specifica decisione assunta. L'articolo 15 GDPR, infatti, sancisce il diritto dell'interessato di richiedere, *in ogni momento*, l'accesso a informazioni relative all'esistenza di un trattamento automatizzato *ex* art. 22 GDPR e, almeno nei casi di cui ai paragrafi 1 e 4, il diritto ad avere informazioni significative sulla logica utilizzata[394].

L'osservazione per cui l'aver mantenuto nell'articolo 15 GDPR, che disciplina un diritto di accesso esercitabile anche *ex post* rispetto all'assunzione di una decisione automatizzata, lo stesso linguaggio utilizzato negli articoli 13 e 14 GDPR che invece disciplinano meri doveri di notifica (per definizione *ex ante*), crei delle ambiguità interpretative che sarebbe stato opportuno evitare è assolutamente condivisibile. Non lo è altrettanto dedurre da tale ambigua identità linguistica che, ove l'interessato eserciti il diritto di accesso *ex* art. 15 GDPR dopo che la decisione sia assunta, quest'ultimo possa comunque ottenere una descrizione meramente astratta della stessa, senza che il titolare sia tenuto a prendere minimamente in considerazione le specifiche circostanze del caso[395].

Tale conclusione, infatti, oltre che logicamente poco convincente, è chiaramente confutata dal considerando 60, ove viene chiarito come "i principi del trattamento corretto e trasparente implicano che […] il titolare del trattamento […fornisca…] all'interessato eventuali ulteriori informazioni […], prendendo in considerazione le *circostanze e [il] contesto specifici* in cui i dati personali sono trattati". Peraltro, lo stesso considerando 71

[394] In senso analogo, si sono espressi anche MALGIERI e COMANDÈ, i quali hanno fatto notare come che mentre gli Articoli 13 para 1 lett. c e 14 para 1 lett. c menzionano l'obbligo del titolare di informare l'interessato circa "le finalità del trattamento cui sono destinati i dati personali", l'Articolo 15 para 1 lett. a riformula la disposizione limitandosi a sancire l'obbligo di rendere note "le finalità del trattamento". Peraltro, continuano gli Autori, che l'Articolo 15 sia formulato in modo temporalmente neutrale è confermato nella parte in cui sancisce il diritto degli interessati a ottenere l'accesso alle informazioni relative ai "destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati." Infine, si fa notare che, se l'espressione "conseguenze previste" può richiamare l'idea di una valutazione compiuta *ex ante* ed in linea generale ed astratta, il riferimento alla "logica utilizzata", al contrario, non può che rievocare una ricostruzione fatta *ex post*, a processo decisionale concluso. ID., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243, 255. Cfr. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer, Berlino, 2017, 79.

[395] Più radicalmente, criticano l'utilità stessa di distinguere tra una spiegazione *ex ante* ed una *ex post* ai fini del riconoscimento dell'esistenza di un diritto ad una spiegazione ai sensi del GDPR, A.D. SELBST e J. POWLES, Meaningful Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017, 238.

puntualizza che "in ogni caso", il trattamento automatizzato a fini decisionali dovrebbe essere subordinato a garanzie adeguate, tra cui il diritto di ottenere una spiegazione della decisione conseguita *dopo* tale valutazione [umana]" e che il titolare del trattamento dovrebbe mettere in atto misure tecniche e organizzative al fine di minimizzare il rischio di errori ed effetti discriminatori "tenendo in considerazione le *circostanze e il contesto specifici*".

In ultima battuta, Wachter *et al*. ritengono che l'assenza del diritto ad una spiegazione *ex post* sia ulteriormente dimostrata, sempre in prospettiva storica, dalle difformi scelte legislative operate dagli Stati membri in fase di recepimento dell'analoga previsione contenuta nel previgente articolo 15 Dir. 95/46/CE. L'ambiguità linguistica fin qui sottolineata ed ereditata dalla previgente Direttiva, sostengono gli Autori, avrebbe consentito a Stati come Francia, Regno Unito e Germania di negare esplicitamente la necessità di divulgare descrizioni relative al funzionamento del software, al codice sorgente, al peso attribuito alle singole variabili prese in considerazione, ammettendo più limitate descrizioni astratte della logica seguita dal c.d. "*decision tree*". Tali soluzioni normative risponderebbero principalmente all'esigenza di bilanciare i diritti informativi dei soggetti interessati con la disciplina sulla protezione dei *trade secret*, nonché a quella di evitare che un'eccessiva trasparenza sul processo decisionale automatizzato consenta agli interessi di manipolarne i risultati[396].

Sebbene, come si vedrà meglio nel prosieguo, entrambe queste preoccupazioni siano tutt'ora condivise dal legislatore eurounitario, neppure quest'ultima argomentazione appare sufficiente ad escludere il diritto dei soggetti interessati di ottenere informazioni più specifiche sull'iter logico che ha condotto alla decisione.

Innanzitutto, le stesse analisi comparative sull'attuazione della Direttiva Madre citate dagli Autori (condotte agli albori dello scorso decennio), mettevano in guardia sull'insufficienza di misure normative "minime" come il mero diritto di non essere

[396] SANDRA WACHTER, BRENT MITTELSTADT e LUCIANO FLORIDI, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7, *International Data Privacy Law*, 2, 2017, 76, 85-87. Cfr. D. KORFF, *New Challenges to Data Protection Study - Country Report: Germany* (European Commission DG Justice, Freedom and Security 2010), 27; ID., *New Challenges to Data Protection Study – Country Report: France* (European Commission DG Justice, Freedom and Security 2010), 27; *UK Data Protection Act* 1998 Sec. 7(1)(d). Cfr. L. A. BYGRAVE, Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, 17, *Computer Law & Security Report*, 2001, 17-24.

sopposti ad una decisione automatizzata, ed invitavano l'allora Gruppo di lavoro articolo 29 ad intervenire con urgenza sul dettato della disposizione per chiarirne la portata, la cui importanza sarebbe senz'altro cresciuta esponenzialmente nel prossimo futuro in virtù della sempre più diffusa adozione di processi decisionali basati su cc.dd. "*computer-generated profiles*"[397]. Peraltro, che tale ricostruzione risulti del tutto anacronistica è dimostrato dal riferimento alla sufficienza della descrizione della logica seguita dal "*decision tree*", tecnica di Intelligenza Artificiale caratterizzata dalla sua intrinseca interpretabilità, principalmente attribuibile alla relativa semplicità delle analisi dati che consente di eseguire, non paragonabili alla complessità e intrinseca opacità delle tecniche di *deep machine learning* oggi diffusamente utilizzate[398].

In secondo luogo, la scelta per lo strumento legislativo del Regolamento testimonia la volontà di armonizzare il livello di tutela in materia di protezione dei dati personali, proprio al fine ultimo di superare le difformità normative rese possibili dal margine di discrezionalità attuativa lasciato ai legislatori nazionali dalla previgente Direttiva.

Infine, seppure con risultati oggettivamente ancora non pienamente soddisfacenti, il linguaggio del GDPR ha indubbiamente specificato e integrato i doveri informativi di cui al previgente articolo 15 Dir. 95/46/CE. Il mero riferimento al diritto di ottenere la "conoscenza della logica applicata nei trattamenti automatizzati", ad esempio, è stato sostituito dall'obbligo del titolare di fornire all'interessato "informazioni significative" su tale logica. Per di più, la disciplina delle "appropriate misure" a tutela dei soggetti

[397] Così D. KORFF, per il quale "[*i*]*ncreased, and increasingly automated analyses of ever-increasing, and ever-more-easily-accessible data carry the risk of individuals becoming mere objects, treated (and even discriminated against) on the basis of computer-generated "profiles", probabilities and predictions, with little or no possibility to counter the underlying algorithms. Unless strong data protection is maintained, decisions with "significant effect" (such as a decision to deny you a job, or to not even invite you for an interview; to be stopped at a border, and possibly denied entry into a country; to be subjected to intrusive surveillance, and possibly arrested, etc.) will increasingly be taken "because the computer said so" - without even the officials or staff carrying out the decision able to fully explain why. The new technologies inherently tend to shift the balance of power away from the individual towards those who hold data on them: the terms "data subject" and "controller" are gaining deeper, more sinister meaning*." ID., *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments* (European Commission DG Justice, Freedom and Security 2010), 17.

[398] Per una interessante classificazione dei processi decisionali sostanziali e processuali, così come della distinzione tra quelli algoritmici e non, ovvero tra decisioni cc.dd. *rule-based* e *law-based* si veda M. BRKAN, Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, 11, *International Journal of Law and Information Technology*, 2019, 1-31. Cfr. T. ZARSKY, The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making, 41, *Science, Technology, & Human Values*, 2016, 118–32.

interessati sottoposti a processi decisionali automatizzati oggi contenuta nell'articolo 22 para 3 GDPR, così come il riferimento al diritto di ottenere una spiegazione della decisione automatizzata di cui al considerando 71 GDPR, non trovano nessun precedente nel testo della Direttiva Madre[399].

Alla luce delle considerazioni sin qui svolte, quindi, si condivide la posizione di chi come Selbst e Powles ha ritenuto la tesi di Wachter, Mittlestad e Floridi una "*overreaction*" all'intuizione di Goodman e Flaxman, suscettibile di distorcere il dibattito in materia. Ciò in quanto, si fa correttamente notare, a dispetto di quanto il titolo del contributo possa far pensare, Wachter *et al.* possono sostenere l'inesistenza di un diritto ad una spiegazione solo ed esclusivamente nella misura in cui lo identificano con un diritto una descrizione *ex post* della specifica decisione automatizzata. Tale conclusione, tuttavia, non riguarda la nozione di "spiegazione" che, seppure in misura attenuata, viene comunque riconosciuta ai soggetti interessati, quanto la portata della nozione di "informazioni significative" sulla logica utilizzata[400].

Il vero cuore del problema, quindi, al quale verrà dedicato il prossimo paragrafo, consiste nello stabilire la quantità e qualità delle informazioni che il titolare del

[399] Cfr. G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243 ss; L. EDWARDS e M. VEALE, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017, 39; B. LEPRI, J. STAIANO, D. SANGOKOYA, E. LETOUZÉ, e NURIA OLIVER, The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, Studies in *Big Data*, Vol. 11, Berlino, Springer, 2017, 5; W. EASTERLY, *The Tyranny of Experts. Economists, Dictators, and the Forgotten rights of the Poor*, Basic Books, New York, 2014, 286; S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, Roma, 2014, 37-40; M. ANNANY e K. CRAWFORD, Seeing Without knowing: limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 973-989.

[400] A.D. SELBST e J. POWLES, Meaningful Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017, 238. Cfr. M. ANANNY e K. CRAWFORD, Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 2018, 973; J. BURRELL, How the machine 'thinks': understanding opacity in machine learning algorithms, 3, *Big Data & Society*, 1, 2016, 1-12; D.K. CITRON, Technological due process, 85, 2007, *Wash.UL Rev*., 1249; L. EDWARDS e M. VEALE, Enslaving the algorithm: from a "right to an explanation" to a "right to better decisions"?, 16, *IEEE Security & Privacy*, 3, 2018, 46-54; K. FINK, Opening the government's black boxes: freedom of information and algorithmic accountability, 21, *Information, Communication & Society*, 10. 2018, 1453; R. GUIDOTTI *et al*., A survey of methods for explaining black box models, 51, *ACM Computing Surveys (CSUR)*, 5, 2018, 93; J.A. KROLL *et al*., Accountable algorithms, 165, *University of Pennsylvania Law Review*, 2016, 633-705; O. TENE e J. POLONETSKY, Taming the Golem: Challenges of ethical algorithmic decision-making, 19, *NCJL & Tech*., 2017, 125 A.D. SELBST e S. BAROCAS, The Intuitive Appeal of Explainable Machines, 87, *Fordham L. Rev*, 3, 2018, 1085.

trattamento è tenuto a condividere con il soggetto interessato ai sensi del combinato disposto degli articoli 13-15 e 22 GDPR.

2.4.1. La spiegazione "significativa"

Dimostrata l'esistenza del diritto ad una spiegazione, l'analisi prosegue con una ricognizione dei requisiti formali e contenutistici della stessa, al fine ultimo di avanzare una proposta di formulazione che sia compatibile con l'attuale quadro normativo e tecnologico.

Sotto il primo aspetto, è indiscutibile che da un punto di vista formale "tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 […] [debbano essere fornite all'interessato] in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro […]"[401]. A tal proposito, infatti, il Regolamento puntualizza come la previsione di doveri informativi (tanto di notifica *ex ante ex* artt. 13-14 GDPR, quanto quelli di comunicazione su richiesta *ex* art. 15 GDPR) risponda all'esigenza di "garantire un trattamento corretto e trasparente", dove la liceità, trasparenza e correttezza sono valutate "nei confronti dell'interessato"[402].

Dal punto di vista funzionale, invece, è altrettanto pacifico che il titolare ha il dovere di "agevola[re] l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22"[403]. In particolare, le "misure appropriate" che il titolare è tenuto ad adottare ove si

[401] GDPR, Articolo 12 para 1.

[402] GDPR, articolo 5 para 1 lett. a. Sulla necessità di ridurre i calcoli del sistema di IA ad una forma comprensibile dagli umani si veda Para 12, sezione "principi etici" della Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)). Particolare attenzione al rischio di implementare forme di trasparenza fallaci perché volte a fornire troppo complesse o troppo dettagliate per essere intelligibili dall'utente medio si vedano le osservazioni già formulate in C. TABARRINI, Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019, 555 ss, spec. nt. 38 ove vengono richiamati gli analoghi timori espressi da F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015, 16 e O. BEN-SHAHAR e C.E. SCHNEIDER, *More Than You Wanted to Know. The Failure of Mandated Disclosure*, Princeton University Press, Princeton, 2014, 55ss.. Cfr. M. ANNANY e K. CRAWFORD, Seeing Without knowing: limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 973-989; F.H. CATE, *Big Data* consent and the future of data protection in C.R. SUGIMOTO, H.R. EBIKA, M.MATTIOLI (a cura di), *Big Data is not a Monolith*, MIT Press, Cambridge (MA), 2016, 3; R. MOMBERG, *Standard Terms and Transparency in Online Contracts*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, cit., 201.

[403] GDPR, Articolo 12 para 2. Cfr. F. PIRAINO, Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, cit., 395; F. CALISAI, *I diritti dell'interessato*, in V. CUFFARO, R.

avvalga di decisioni automatizzate fondate sulla necessità contrattuale ovvero sul consenso dell'interessato, sono finalizzate a "tutelare i diritti, le libertà e i legittimi interessi dell'interessato". Allo scopo, come già accennato, il legislatore ha avuto cura di chiarire ulteriormente la portata di tale obbligo, specificando come siffatte "garanzie adeguate" dovrebbero comprendere "almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione"[404], nonché "di ottenere una *spiegazione* della decisione conseguita *dopo* tale valutazione [umana]"[405].

In prospettiva organizzativa, infine, sappiamo che tali doveri dovrebbero essere assolti dal titolare "tenendo in considerazione le *circostanze e il contesto specifici* in cui i dati personali sono trattati" ed avvalendosi di "misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano *rettificati* i fattori che comportano *inesattezze* dei dati e sia *minimizzato* il rischio di *errori* e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che *impedisca tra l'altro effetti discriminatori* nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti"[406].

Alla luce del dato normativo sin qui analizzato, è quindi possibile escludere qualsivoglia dubbio esegetico circa le circostanze per cui: (i) la trasparenza e l'intellegibilità del trattamento debbono essere parametrate alla capacità di comprensione dei soggetti interessati[407]; (ii) l'adempimento dei doveri informativi è funzionale a consentire l'esercizio del diritto dell'interessato *ex* artt. 15 e 22 para 1 e 4 GDPR, nonché

D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 336.

[404] GDPR, articolo 22 para 3.

[405] GDPR, considerando 71.

[406] GDPR, cons. 71. Sui rischi di discriminazione si veda anche M. RHOEN e Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018, 140.

[407] Cfr. B. LEPRI, J. STAIANO, D. SANGOKOYA, E. LETOUZÉ, e NURIA OLIVER, The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, Studies in *Big Data*, Vol. 11, Berlino, Springer, 2017, 5; W. EASTERLY, *The Tyranny of Experts. Economists, Dictators, and the Forgotten rights of the Poor*, Basic Books, New York, 2014, 286 e S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Editori Laterza, Roma, 2014, 37-40.

del diritto a contestare la decisione così assunta *ex* art. 22 para 2 lett. a e c GDPR[408]; (iii) l'osservanza di tali doveri richiede l'implementazione di misure organizzative tali da consentire al titolare di rettificare i fattori fonti di errori, minimizzare inesattezze nei dati nonché prevenire effetti discriminatori; (iv) ciascuna di queste misure deve poter operare tenendo in considerazione le circostanze specifiche in cui sono trattati i dati.

Vagliando le principali proposte dottrinali formulate, è quindi nel rispetto dei confini normativi così ricostruiti che si tenterà di sciogliere i quesiti applicativi posti dall'esegesi del dovere di fornire all'interessato informazioni concernenti la "logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento"[409]. Ci si chiede, infatti, quale grado di *disclosure* il legislatore eurounitario abbia inteso imporre ai titolari del trattamento con tale formulazione[410].

Guardando alla spiegazione in prospettiva funzionale (i.e. "come strumento per aiutare il soggetto interessato ad agire piuttosto che semplicemente a capire"), ad esempio, Wachter, Mittelstadt e Russell hanno avanzato la tesi della c.d. "*unconditional counterfactual explanation*"[411]. Quest'ultima, offrendo una mera descrizione del rapporto *input-output*, presenterebbe il vantaggio di evitare di aprire la c.d. *black box* tentando di tradurre in termini umanamente comprensibili la complessa logica algoritmica seguita dal

[408] Nonostante la chiarezza del dettato normativo questa soluzione non sembrerebbe essere condivisa da WACHTER *et al*. i quali, come si vedrà meglio *infra* nel testo, fondano la sostenibilità giuridica della tesi di una c.d. spiegazione controfattuale sulla asserita assenza di un collegamento tra il diritto ad una spiegazione e il diritto di contestare la decisione, ovvero tra quest'ultimo e i doveri del titolare di adottare meccanismi di trasparenza del trattamento e di notifica. Ne conseguirebbe che i titolari del trattamento non avrebbero un obbligo giuridico di fornire all'interessato informazioni particolarmente utili affinché il soggetto interessato possa esercitare i propri diritti. Utilizzando le parole degli Autori, "sebbene una spiegazione potrebbe essere utile, essa non appare intesa come una precondizione per contestare la decisione". S. WACHTER, B. MITTELSTADT, C. RUSSELL, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018, 35-40 (in realtà pag sono 842-887); A. RAI, Explainable AI. From Black Box to Glass Box, in Journal of the Academy of Marketing Science, 48, 2020, 137 ss; T. WISCHMEYER, *Artificial Intelligence and Transparency: Opening the Black Box*, in T. WISCHMEYER, T. RADEMACHER (a cura di), *Regulating Artificial Intelligenc*e, Springer, Cham, 2020, 75 ss.

[409] GDPR, considerando 63.

[410] Cfr. D.LEWANDOWSKI, Is Google Responsible for Providing Fair and Unbiased Results?, in M. TADDEO, L. FLORIDI (a cura di), *The Responsibilities of Online Service Providers*, Law, Governance and Technology Series, Vol. 31, Springer, New York, 2017, 62; T. GILLESPIE, The relevance of algorithms, in T. GILLESPIE, P.J. BOCZKOWSKI, & K.A. FOOT (a cura di), *Media Technologies: Essays on Communication, Materiality, and Society*, MIT Press, Cambridge (MA), 168.

[411] Nelle parole degli Autori, una siffatta spiegazione potrebbe, ad esempio, assumere la seguente formulazione "*You were denied a loan because your annual income was £30,000. If your income had been £45,000, you would have been offered a loan*". S. WACHTER, B. MITTELSTADT, C. RUSSELL, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018, 5.

sistema per addivenire ad una decisione. Modellando l'approccio sul funzionamento delle tecniche informatiche di "*adversarial perturbation*", tale tipologia di spiegazione si tradurrebbe nell'indicare al soggetto interessato il più piccolo cambiamento che quest'ultimo dovrebbe/avrebbe potuto apportare alla sua condizione iniziale per ottenere la soluzione desiderata[412].

Come gli Autori abbiano potuto ritenere una tale soluzione compatibile con il quadro normativo di cui in premessa si può comprendere nella parte in cui ne viene negata l'esistenza. Wachter *et al*., infatti, muovono dell'assunto per cui "il GDPR non definisce esplicitamente i requisiti che la spiegazione deve rispettare e offre pochi indizi circa l'obiettivo perseguito con la spiegazione delle decisioni automatizzate"[413].

È quindi alla luce di tale presunto silenzio del Regolamento che gli Autori maturano la convinzione dell'adeguatezza delle spiegazioni controfattuali, ritenendole in linea ai tre principali obiettivi che, nell'opinione degli Autori stessi, e a dispetto del dettato normativo, la spiegazione dovrebbe perseguire: (i) capire il perché di una specifica decisione; (ii) offrire le basi per poter contestare esiti a sé sfavorevoli; e (iii) comprendere cosa modificare per ottenere il risultato desiderato in futuro. Ciò in quanto, ammettono gli Autori, "*trust is essential to increase societal acceptance of algorithmic decision making*"[414].

[412] Il c.d. *Adversarial Machine Learning* muove dal problema informatico degli *adversarial examples* (o esempi antagonistici). A seguito dell'ascesa dell'accuratezza delle tecniche di ML, alcuni informatici hanno iniziato ad evidenziare il rischio di manipolare le informazioni in modo da ingannare le reti neurali dei sistemi di ML. In particolare, si tratta di *input* che vengono modificati (ad esempio aggiungendo rumore statistico) apportandovi, fra tutti i cambiamenti possibili, quello più impercettibile ma comunque idoneo a indurre il sistema a ML a produrre un *output* errato. Di qui, l'evidente affinità con la soluzione analizzata nel testo: partendo dall'*output* desiderato, si ricerca il cambiamento più piccolo da apportare agli *input* originariamente impartiti al sistema per ottenerlo. Per ovviare a tale rischiosa sensibilità dei sistemi ML si sta peraltro promuovendo l'adozione di modelli di c.d. *causal reasoning*, volti a "insegnare" ai sistemi di AI a compiere collegamenti causali tali da, ad esempio, prevenire errori nella lettura dei cartelli stradali da parte dei veicoli a guida autonoma. Cfr. S.M. MOOSAVI-DEZFOOLI, A. FAWZI, P. FROSSARD, DeepFool: a simple and accurate method to fool deep neural networks, *arXiv:1511.04599*, 2016; Q. SONG, H. JIN, X. HUANG, X. HU, Multi-Label Adversarial Perturbations, *arXiv:1901.00546*, 2019; J. PEARL, D. MACKENZIE, *The Book of Why: The New Science of Cause and Effe*ct, Basic Books, New York, 2018; T. HAZAN, G. PAPANDREOU, D. TARLOW (a cura di), *Perturbations, Optimization, and Statistics*, MIT Press, Cambridge (MA), 2016.

[413] S. WACHTER, B. MITTELSTADT, C. RUSSELL, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018, 23.

[414] IVI, 4. Cfr. I. MENDOZA e L.A. BYGRAVE, The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer, Berlino, 2017, 97.

Sebbene tali obiettivi non siano poi distanti da quelli ricostruibili dalla normativa, non si può dire altrettanto dei risultati che verrebbero concretamente raggiunti con tale soluzione.

Rispetto al primo obiettivo, Wachter *et al.* sostengono che, nella misura in cui il GDPR non imporrebbe una descrizione della logica interna ma del solo funzionamento astratto del sistema[415], l'obbligo di fornire "informazioni significative sulla logica utilizzata" sarebbe soddisfatto dall'indicazione delle categorie di dati utilizzate per creare un profilo, della fonte di tali informazioni e delle ragioni per cui tali elementi sono considerati rilevanti, e non una dettagliata descrizione tecnica del funzionamento dell'algoritmo o del sistema di *machine learning*[416].

Ciò che gli Autori sembrerebbero quindi voler affermare, negando l'esistenza di un diritto ad una spiegazione, intesa come diritto a conoscere la logica interna del sistema decisionale automatizzato, è, più precisamente, la non configurabilità di un diritto di accesso al codice sorgente dell'algoritmo, alla sua formula, al completo set di variabili utilizzate e il loro peso, nonché alle informazioni relative ai gruppi inferiti dall'analisi dei dati[417].

A dispetto dei menzionati dubbi sollevati rispetto al percorso esegetico che ha condotto a tale conclusione, quest'ultima è in parte condivisibile. Come si vedrà meglio

[415] È interessante notare come gli Autori richiamino a supporto della loro posizione le Linee guida sul processo decisionale automatizzato elaborate dal Gruppo di Lavoro Articolo 29, sostenendo che quest'ultimo condivida l'idea per cui l'articolo 15 para 1 lett. h GDPR non crei un diritto ad una spiegazione individuale implicante la comprensione della logica interna dell'algoritmo, ma soltanto informazioni circa la generica funzionalità del sistema. In realtà, nelle parole del Gruppo di Lavoro, "[i]l regolamento impone al titolare del trattamento di fornire informazioni significative sulla logica utilizzata, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo." A tal fine, facendo l'esempio dell'utilizzo di formule di *credit scoring*, il gruppo di lavoro puntualizza che il titolare dovrebbe fornire dettagli "sulle principali caratteristiche considerate per giungere alla decisione, sulla fonte di tali informazioni e sulla loro importanza". GRUPPO DI LAVORO ARTICOLO 19, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679* adottate il 3 ottobre 2017 (versione emendata e adottata in data 6 febbraio 2018) (WP 251 rev.01), 28. Sembrerebbe, quindi, che il Gruppo di lavoro articolo 29 effettivamente neghi l'esistenza di una spiegazione della logica interna, nella misura in cui quest'ultima viene identificata nella descrizione tecnica del funzionamento dell'algoritmo. Come si vedrà meglio nel proseguo del paragrafo, tuttavia, il fatto che la *disclosure* dell'algoritmo non sia oggettivamente il più efficiente metodo di apertura della *black box*, non implica l'assenza di altre soluzioni, né il venir meno dell'esigenza di individuarle.

[416] S. WACHTER, B. MITTELSTADT, C. RUSSELL, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018, 25. Sull'analogo concetto di spiegazione c.d. "*sensitivity-based*" si veda L. EDWARDS e M. VEALE, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017, 58.

[417] IVI, 34.

nel prosieguo, l'accesso al codice sorgente o all'algoritmo entrerebbe in inevitabile contrasto con la disciplina sulla protezione del software e dei segreti commerciali[418]. Contrasto, peraltro, del tutto evitabile poiché tale forma di conoscenza non può che risultare incompatibile ai principi di trasparenza e comprensibilità come ricostruiti in premessa. È evidente, infatti, che il soggetto interessato poco possa dedurre dalle complesse formule matematiche circa i motivi di un'eventuale contestazione della decisione automatizzata per tal via assunta[419].

Rinviando al prosieguo del paragrafo la questione dell'accesso ai profili e ai gruppi inferiti dai dati, merita qui ulteriore approfondimento, invece, la conclusione per cui l'interessato non avrebbe diritto ad accedere all'intero set di variabili utilizzate e di conoscerne il relativo peso.

In primo luogo, si ritiene opportuno mettere in evidenza come il diritto dell'interessato di avere accesso alle "categorie di dati" oggetto di trattamento *ex* art. 15

[418] Sulla diversa posizione giurisprudenziale assunta dal Consiglio di Stato, sez. VI, Sent. n.2270 dell'8 aprile 2019 e dalla sez. III-*bis* TAR Lazio con la sentenza n. 3769/2017 rispetto al diniego opposto dal Ministero Italiano dell'Istruzione alla richiesta di accesso al codice sorgente del software utilizzato per prendere decisioni interamente automatizzate riguardanti il collocamento sul territorio del personale docente, avanzata da un'associazione sindacale rappresentativa di insegnanti, si veda meglio *infra* §2.5, nonché quanto già osservato in C. TABARRINI, Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019, 555 ss. Cfr. B. DANIEL MITTELSTADT, P. ALLO, M. TADDEO, S. WACHTER e L. FLORIDI, The Ethics of Algorithms: Mapping the Debate, 2, *Big Data & Society*, 2016, 1-21; F. BRAVO, Trasparenza del codice sorgente e decisioni automatizzate, *Diritto dell'Informazione e dell'Informatica*, 4, 2020, 693 ss; E. PROSPERETTI, Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del Tar Lazio, in *Diritto dell'Informazione e dell'Informatica*, 2019, 979 ss; M. FERRARI, L'uso degli algoritmi nell'attività amministrativa discrezionale, in *Il diritto degli affari*, 2020, 1, 1 ss; A.G. OROFINO, G. GALLONE, L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione, in *Giur. it.*, 2020, 1738 ss; F. BRAVO, Access to source code of proprietary software used by public administrations for automated decision-making. What proportional balancing of interests?, in *European Review of Digital Administration & Law (Erdal)*, 2020, 1-2, 157 ss; E. FALLETTI, Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, in *Diritto dell'Informazione e dell'Informatica*, 2020, 169 ss; C. STRINATI, Algoritmi e decisioni amministrative, *Il Foro Amministrativo*, 7, 2020, 1591ss; E. CARLONI, I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo, in *Diritto Amministrativo*, 2, 2020, 271 ss; F. DE LEONARDIS, Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione, in E. CALZOLAIO (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Padova, Wolter Kluwers Cedam, 2020, 137 ss.

[419] In senso analogo si è espressa la Commissione Europea per l'Efficienza della Giustizia del Consiglio d'Europa (CEPEJ) nella *European Ethical Charter on the use of artificial intelligence in judicial systems and their environment*, adottata in occasione della 31esima sessione plenaria (Strasburgo, 3-4 dicembre 2018), spec. il quarto principio di trasparenza, dell'imparzialità e dell'equità. Cfr. *Algorithms and Human Rights. Studies on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications*", DGI (2017)12 (CONSIGLIO D'EUROPA, marzo 2018) ove vengono richiamate le analoghe osservazioni compiute nel Report Villani, "*AI for humanity*" elaborato in esecuzione del compito affidatogli dal primo ministro francese, così come nel report della House of Lords, "*AI in the UK: ready, willing and able*?", spec. para 92, 96-99. Si veda anche D.E. POZEN, Transparency's Ideological Drift, 128, *Yale L. J.*, 2018, 100 ss.

para 1 lett. b GDPR e di conoscere la ragione per cui tali informazioni siano rilevanti (*rectius* coerenti con le finalità del trattamento) *ex* art. 15 para 1 lett. a prescindono dall'esistenza di un processo decisionale automatizzato, e nulla hanno a che vedere con il diritto ad avere una spiegazione della decisione algoritmica e quindi a conoscerne la logica, così come sancito dagli articoli 15 para 1 lett. h e 22 para 3 GDPR[420].

In questi termini, quindi, la tesi della spiegazione controfattuale nulla aggiunge ai doveri informativi pacificamente riconducibili al GDPR e svuota di portata concreta il diritto ad una spiegazione (seppure generica e inerente alla mera funzionalità stratta del sistema), identificandolo con i primi.

La conclusione può essere in parte diversa, invece, ove si identifichi il contenuto della spiegazione con la descrizione delle variabili utilizzate, intese come i parametri che hanno guidato la logica algoritmica. Anche qui, tuttavia, nulla si aggiunge al percorso ermeneutico volto a ricostruire la portata effettiva del diritto, lasciando ancora una volta irrisolto il quesito relativo al *quantum e quomodo* della *disclosure*. In particolare, come accennato, la dottrina si è interrogata sul se una descrizione, per poter assurgere a informazione "significativa"[421] e "specifica"[422], debba riguardare la singola decisione, individualmente considerata, e debba altresì prendere in considerazione l'intera pletora di criteri indicati (e molto spesso autonomamente sviluppati) dal sistema per addivenire alla determinazione[423].

---

[420] Cfr. F. CALISAI, *I diritti dell'interessato*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 338 ss; F. DI RESTA, *La nuova 'Privacy europea': i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore, Torino, 2018, 65 ss; A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 182 ss; D. MONTANARO, *Il diritto di accesso ai dati personali e il diritto di rettifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019, 187 ss; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli Editore, Torino, 2018, 87 ss; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679*, Vol. II, Giappichelli Editore, Torino, 2016, 86 ss; E. LUCCHINI GUASTALLA, *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019, 78ss.

[421] Come richiesto dagli articoli 13 para 2 lett. f, 14 para 2 lett. g e 15 para 1 lett. h GDPR.

[422] Come richiesto dal considerando 60 e 71 GDPR.

[423] Si veda, fra gli altri, G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243 ss; L. EDWARDS e M. VEALE, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017, 39; S. WACHTER, B. MITTELSTADT, C. RUSSELL, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018, 35-4; A.D. SELBST e S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1085; A.D. SELBST e J. POWLES, Meaningful

Con riguardo a tale ultimo interrogativo, una risposta affermativa sembrerebbe venire dal Gruppo di Lavoro articolo 29 nella misura in cui ha ribadito come "[l]'interessato sarà in grado di contestare una decisione o esprimere il proprio parere soltanto se comprende pienamente come è stata presa la decisione e su quali basi"[424]. Tale comprensione piena, sembrerebbe supportare la tesi del diritto ad una altrettanto piena *disclosure*. Al contempo, tuttavia, è proprio lo stesso Gruppo di Lavoro a puntualizzare come, sebbene le informazioni significative debbano essere "sufficientemente complete affinché l'interessato possa comprendere i motivi alla base della decisione", tale requisito debba ritenersi soddisfatto ove il titolare "fornisc[a] dettagli sulle *principali* caratteristiche considerate per giungere alla decisione, sulla fonte di tali informazioni e sulla loro importanza"[425].

Una tale soluzione interpretativa sembrerebbe confermata anche dai nuovi obblighi di trasparenza introdotti dalla direttiva 2019/2161/UE[426] che, emendando la direttiva 2011/83/UE, ha previsto specifici doveri supplementari di informazione precontrattuale per i contratti conclusi nei mercati online. In particolare, in virtù del nuovo articolo 6 *bis* "[p]rima che un consumatore sia vincolato da un contratto a distanza, o da una corrispondente offerta, su un mercato online, il fornitore del mercato online, ferma restando la direttiva 2005/29/CE, indica al consumatore anche, in maniera chiara e comprensibile e in modo appropriato al mezzo di comunicazione a distanza: a) informazioni *generali*, rese disponibili in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentate le offerte, in merito ai *principali* parametri che determinano la classificazione, quale definita all'articolo 2, paragrafo 1, lettera m), della direttiva 2005/29/CE, delle offerte presentate

Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017, 238; J. BURRELL, How the machine 'thinks': understanding opacity in machine learning algorithms, 3, *Big Data & Society*, 1, 2016, 1-12; R. GUIDOTTI *et al.*, A survey of methods for explaining black box models, 51, *ACM Computing Surveys (CSUR)*, 5, 2018, 93ss.

[424] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 31.

[425] IVI, 29.

[426] La direttiva 2019/2161/UE che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE e 21011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori (d'ora in avanti Direttiva Omnibus). La normativa in questione, insieme al regolamento (UE) 2019/1150 è parte del c.d. *New Deal for Consumers* i cui obiettivi sono: (i) estendere i diritti dei consumatori al contesto dei servizi digitali "gratuiti"; (ii) rafforzare gli standard di trasparenza online, in particolare rispetto alla personalizzazione dei prezzi e dei risultati dei motori di ricerca; (iii) garantire un maggiore rispetto della normativa, inasprendo le sanzioni e prevendo meccanismi di reclamo e azione di classe più effettivi.

al consumatore come un risultato della sua ricerca e all'*importanza relativa di tali parametri rispetto ad altri parametri*".

È noto, infatti, come nell'era del c.d. "capitalismo di sorveglianza"[427] la personalizzazione dei prezzi, così come dei risultati delle ricerche online, operata sulla base di processi decisionali automatizzati *ex* art. 22 GDPR incida notevolmente sulle scelte dei consumatori, condizionandone il comportamento[428]. Allo stesso tempo, l'utilizzo di algoritmi di classificazione sempre più complessi da parte dei fornitori di motori di ricerca e di altre piattaforme che consentono la ricerca di prodotti e servizi, ha creato un vuoto di responsabilizzazione e prevedibilità del funzionamento di tali procedure di *ranking* subìto anche dagli stessi utenti commerciali, la cui capacità di raggiungere la clientela sempre più dipende dal posizionamento ottenuto dai loro prodotti e servizi su tali piattaforme[429].

I termini e le condizioni di utilizzo di molte piattaforme online, infatti, offrono una descrizione dei parametri utilizzati per la classificazione vaga ed opaca. Tale carenza

---

[427] Così si esprime Shoshana Zuboff, secondo la quale "*Surveillance capitalism is the puppet master that imposes its will through the medium of the ubiquitous digital apparatus. I now name the apparatus Big Other: it is the sensate, computational, connected puppet that renders, monitors, computes, and modifies human behavior. Big Other combines these functions of knowing and doing to achieve a pervasive and unprecedented means of behavioral modification. Surveillance capitalism's economic logic is directed through Big Other's vast capabilities to produce instrumentarian power, replacing the engineering of souls with the engineering of behavior.*" ID., *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019, 353. Cfr. R. TAYLOR, No Privacy Without Transparency, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura si) *Data Protection and Privacy: The Age of Intelligent Machines,* Hart Publishing, Oxford, 2017, 77.

[428] Si parla in questo senso di trappola dell'autonomia "perché [se] una persona non è consapevole dei profili che le sono attribuiti potrebbe essere indotta ad agire in modo diverso da ciò che avrebbe scelto qualora li avesse conosciuti. […] La mia autonomia è elusa e la mia volontà indebolita ogni volta in cui non sono consapevole delle informazioni che vengono utilizzate." M. HILDEBRANDT, The Dawn of a Critical Transparency Right for the Profiling Era, in J. BUS, M. CROMPTON, M. HILDEBRANDT, G. METAKIDES (a cura di), *Digital Enlightenment Yearbook 2012*, IOS Press, Amsterdam, 49. Cfr. F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015, 5; A. OTTOLIA, *Big Data* e Innovazione Computazionale, Quaderni di Aida n.28, Torino, Giappichelli Editore, 2017, 202; M. MATTIOLI, Disclosing *Big Data*, in *Minnesota Law Review*, 99, 2014, 2, 535ss; T.Z. ZARSKY, "Mine your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, 5, *Yale Journal of Law and Technology*, 1, 1-56.

[429] *Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services* (CONSIGLIO DELL'UNIONE EUROPEA, Bruxelles 30 aprile 2018) 2018/0112 (COD), 12-16. In particolare, il Consiglio riporta come "[*i*]*n some of the biggest EU Member States, online platforms (as defined in this Impact Assessment) already account for a share of over 40% of total desktop Internet traffic in the e-commerce and hospitality sectors (see section 7.2.5. of the Annexes to this report). The largest part of this share (70%-80%) is accounted for by direct Internet traffic and therefore does not rely on referrals by online general search engines. These figures underline the crucial market gateway that online platforms represent for business users.*"

di trasparenza nei rapporti P2B, associata alla rapidità con cui tali parametri tendono a cambiare, ha alimentato i timori degli utenti commerciali di essere vittime di forme arbitrarie di c.d. *dimming*[430]. L'oscurità dei criteri seguiti nella classificazione, peraltro, tende a rimanere incensurata nella misura in cui lo squilibrio di potere tra le piattaforme e gli utenti commerciali fa sì che questi ultimi si astengano dal presentare reclami per timore di ritorsioni in termini di retrocessione o esclusione dalla piattaforma[431].

È in questo contesto, quindi, che il legislatore eurounitario ha ritenuto necessario rinforzare i doveri di trasparenza introdotti dalla direttiva Omnibus verso i consumatori in punto di criteri di classificazione dei risultati di ricerche online, con la previsione di analoghi doveri informativi negli specifici rapporti P2B, disciplinati dal regolamento (UE) 2019/1150[432].

Lo scopo perseguito da entrambe le normative è quello di rendere più prevedibile il processo decisionale algoritmico che porta la piattaforma a fissare un determinato ordine dei risultati di ricerca, favorendo in tal modo una maggiore responsabilizzazione dei fornitori di motori di ricerca e una maggiore consapevolezza degli utenti commerciali circa le modalità per influenzare tali risultati[433]. È proprio l'evidente affinità d'intenti che

---

[430] Con tale espressione si intende l'arretramento del ranking di un business operato arbitrariamente da gestori di piattaforme online come forma di ritorsione per determinati comportamenti. Per un'analisi del fenomeno nel settore alberghiero si veda K. DOGGRELL, *Checking Out: What the Rise of the Sharing Economy Means for the Future of the Hotel Industry*, Bloomsbury, Londra, 2020, 117 ss. Di particolare rilievo ai fini dell'analisi qui condotta risulta poi lo studio empirico condotto da M. HUNOLD, R. KESLER e U. LAITENBERGER, dove viene investigata "*the question of whether OTAs condition their rankings of search results on the hotel prices at other OTAs or on the hotels' websites. […], we show that in order to maximize long-term profits, an OTA may also employ a policy whereby it conditions the ranking directly, and possibly more drastically, on whether a hotel is offering lower prices on competing channels*. […] *We find that for a given hotel price at an OTA, a lower price at the other OTA or on the hotel's website leads to a worse ranking position. This suggests that the OTA conditions its recommended ranking on factors that are relevant for the OTA to maximize its profit, but arguably not to maximize the match value of consumers*." ID., *Hotel Rankings of Online Travel Agents, Channel Pricing and Consumer Protection* (DÜSSELDORF INSTITUTE FOR COMPETITION ECONOMICS, settembre 2018), 2-3.

[431] *Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services* (CONSIGLIO DELL'UNIONE EUROPEA, Bruxelles 30 aprile 2018) 2018/0112 (COD), 26. Cfr. M. MIDIRI, Le piattaforme e il potere dei dati (Facebook non passa il Reno), in *Diritto dell'Informazione e dell'Informatica*, 2, 2021, 111 ss.

[432] Regolamento (UE) 2019/1150 del Parlamento Europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, G.U. L 186/57.

[433] In questo senso si esprime chiaramente il Considerando 8 Reg. (UE) 2019/1150 per cui "[t]ali norme dovrebbero anche fornire incentivi adeguati per promuovere l'equità e un'adeguata trasparenza, in particolare riguardo il posizionamento degli utenti titolari di siti web aziendali nei risultati di ricerca generati dai motori di ricerca online." La Commissione europea, inoltre, nel riportare gli esiti di studi statistici sulla trasparenza ha osservato un aumento del 115% della probabilità di acquisti da parte dei consumatori, ove correttamente informati circa i criteri adottati per fissare l'ordine dei risultati di una

la disciplina condivide con le "misure adeguate" di cui all'articolo 22 GDPR, a rendere tale disposto normativo particolarmente rilevante ai fini dell'analisi sin qui condotta. La maggiore precisione mostrata dal legislatore eurounitario nel disciplinare i doveri informativi delle piattaforme *online,* infatti, può aiutare a sciogliere, in prospettiva sistematica, i nodi esegetici che ancora offuscano la nozione di "informazioni significative"[434].

A tal fine, è interessante notare come la direttiva 2019/2161/UE imponga ai "professionisti che permettono ai consumatori di effettuare ricerche di beni e servizi, quali viaggi, alloggi e attività ricreative, offerti da altri professionisti o da consumatori" di "informarli in merito ai *principali parametri* predefiniti che determinano la classificazione delle offerte presentate al consumatore come risultato della sua ricerca e *all'importanza relativa di tali parametri rispetto ad altri parametri*"[435].

Leggendo tale disposizione alla luce dei considerando, si comprende chiaramente come l'obiettivo perseguito con la previsione di un siffatto obbligo informativo sia quello di consentire agli utenti commerciali di comprendere quali aspetti della presentazione dei

ricerca online. *Commission Staff working document-Impact assessment accompanying the document proposals for directives of the European Parliament and of the Council amending Council Directive 93/13/EEC, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules and on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC* (COMMISSIONE EUROPEA, Bruxelles, 11 aprile 2018), SWD(2018) 96 final pt. 1/3, 64. In senso analogo si è espressa anche la Commissione per i trasporti e il turismo la quale, fra le proprie proposte di emendamenti alla Direttiva Omnibus, includeva l'introduzione di un nuovo considerando 6 *bis* in base al quale "i doveri di informazione e trasparenza delle parti coinvolte dovrebbero essere applicati rigorosamente affinché i consumatori possano fidarsi delle piattaforme e delle imprese che le utilizzano e non sia compromessa la loro fiducia nel mercato unico." C. ȚAPARDEL, *Parere della Commissione per i trasporti e il turismo destinato alla Commissione per il mercato interno e la protezione dei consumatori sulla proposta di regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online* (PARLAMENTO EUROPEO, 23 novembre 2018) (2018/0112(COD)).

[434] Che la fattispecie presa in considerazione dalle normative richiamate sia non soltanto affine, ma possa coincidere con i processi decisionali automatizzati aventi ad oggetti dati personali è confermato dal considerando 45 della Direttiva 2019/2161/UE in base al quale i doveri informativi ivi disciplinati "non pregiudica[no] le disposizioni del regolamento (UE) 2016/679, che stabilisce, tra l'altro, il diritto delle persone fisiche di non essere assoggettate a processi decisionali automatizzati relativi alle persone fisiche, inclusa la profilazione".

[435] In senso analogo si esprime anche l'Articolo 3 paragrafo 4 lett. b Direttiva Omnibus, rubricato "Modifiche della direttiva 2005/29/CE", in base al quale "La direttiva 2005/29/CE è così modificata: […] 4) l'articolo 7 è così modificato: [...] b) è inserito il seguente paragrafo: «4 *bis*. Per cui "sono considerate rilevanti le informazioni generali, rese disponibili in un'apposita sezione dell'interfaccia online che sia direttamente e facilmente accessibile dalla pagina in cui sono presentati i risultati della ricerca, in merito ai parametri principali che determinano la classificazione dei prodotti presentati al consumatore come risultato della sua ricerca e all'importanza relativa di tali parametri rispetto ad altri parametri."

loro beni e servizi, ovvero quali caratteristiche inerenti agli stessi, ne hanno influenzato il posizionamento, così da poter sapere dove focalizzare gli sforzi di miglioramento *pro-futuro*. In quest'ottica, la "spiegazione" dovrebbe prendere la forma di una "descrizione ragionata" consistente nell'"identificazione di una serie limitata di parametri maggiormente rilevanti, a partire da un numero possibilmente molto più elevato di parametri che hanno un impatto sul posizionamento"[436].

Tanto nel regolamento (UE) 2019/1150 quanto nella direttiva 2019/2161/UE, inoltre, il legislatore ha voluto chiarire la nozione di "parametro principale" con ciò intendendo ogni "criterio generale, processo, segnale specifico integrato negli algoritmi o ogni altro meccanismo di aggiustamento o di retrocessione utilizzato in connessione con il posizionamento" o "con la classificazione"[437].

A tale esemplificazione, infine, il Regolamento (UE) 2019/1150 aggiunge la specificazione per cui tali informazioni non dovrebbero essere standardizzate, ma differenziate in base agli specifici servizi di intermediazione *online.* Ciò al fine di chiarire come il meccanismo di posizionamento tenga conto "delle caratteristiche dell'effettiva offerta di beni o servizi da parte dell'utente commerciale, e la loro rilevanza per i consumatori degli specifici servizi di intermediazione online". In questo senso, il legislatore offre ulteriori esempi di parametri principali quali: "gli indicatori utilizzati per misurare la qualità dei beni o servizi degli utenti commerciali, il ricorso alle tecniche di *editing* e alla loro capacità di influenzare il posizionamento di tali beni o servizi, la misura dell'impatto del corrispettivo sul posizionamento come pure gli elementi che non si riferiscono al bene o al servizio stesso o vi si riferiscono soltanto in maniera marginale, come le caratteristiche di presentazione dell'offerta online"[438].

[436] Regolamento (UE) 2019/1150 del Parlamento Europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, G.U. L 186/57, Considerando 24.

[437] Direttiva Omnibus, considerando 22 e Reg. (UE) 2019/1150, considerando, 24.

[438] Vale la pena aggiungere, infine, che "per assicurare la prevedibilità per gli utenti titolari di siti web aziendali, la descrizione dovrebbe anche essere tenuta aggiornata, e qualsiasi modifica ai parametri principali dovrebbe essere resa facilmente identificabile." In tal senso, Cons. 25 e 26 reg 2019/1150. Lo stesso concetto è ripetuto nell'articolo 5, rubricato "posizionamento", ai sensi del quale "I fornitori di servizi di intermediazione online stabiliscono nei loro termini e nelle loro condizioni i principali parametri che determinano il posizionamento e i motivi dell'importanza relativa di tali parametri principali rispetto ad altri parametri. I fornitori di motori di ricerca online indicano i principali parametri che, individualmente o collettivamente, sono i più significativi per determinare il posizionamento e specificano l'importanza relativa di tali parametri principali fornendo sui loro motori di ricerca online una descrizione facilmente e

Ulteriori spunti interpretativi sono poi offerti dal regolamento (UE) 2019/1150 circa il grado di specificità della spiegazione. Pur ammettendo, infatti, una descrizione parziale dei criteri utilizzati nel processo decisionale, rimane da chiarire se i doveri informativi di cui agli articoli 13-15 e 22 GDPR debbano o meno essere assolti dal titolare guardando alle specifiche circostanze del caso concreto (spiegazione c.d. *case-based*), ovvero fornendo una descrizione astratta delle generiche funzionalità del sistema (spiegazione c.d. *model-centric)*[439].

Sebbene, come accennato, non sia mancato chi in dottrina ha criticato l'opportunità stessa di operare una tale netta contrapposizione[440], è impossibile formulare un'ipotesi di contenuto della spiegazione senza sciogliere tale quesito interpretativo. Come visto in premessa, infatti, e riconosciuto dallo stesso Gruppo di lavoro articolo 29, "l'articolo 13, paragrafo 2, lettera f), e l'articolo 14, paragrafo 2, lettera g), impongono al titolare del trattamento di fornire informazioni *specifiche* […] sul processo decisionale". Allo stesso modo, sappiamo che le garanzie adeguate di cui all'articolo 22 paragrafo 3 "dovrebbero comprendere la *specifica* informazione all'interessato"[441] e che il principio di correttezza e trasparenza del trattamento impone al titolare di assolvere i propri doveri informativi "prendendo in considerazione le circostanze e del contesto *specifici* in cui i dati personali sono trattati"[442].

Ciononostante, nessun ulteriore supporto ermeneutico è offerto dal GDPR per ricostruire il grado di dettaglio informativo in cui si dovrebbe in concreto tradurre tale requisito della spiegazione. Non si può dire lo stesso, invece, per il regolamento (UE) 2019/1150, il quale al considerando 15 chiarisce che i "termini e le condizioni non si dovrebbero considerare redatti in un linguaggio semplice e comprensibile quando sono vaghi, non specifici e non dettagliati su questioni commerciali importanti e quindi che

pubblicamente accessibile, redatta in un linguaggio semplice e comprensibile. Essi tengono aggiornata tale descrizione."

[439] Una spiegazione modello-centrica è definita come quella spiegazione che, rimanendo indifferente agli *input* e agli *output* specifici del caso concreto, si limita a descrivere l'obiettivo generale sottostante l'intero procedimento algoritmico, la generica classificazione dei dati utilizzati per programmare l'algoritmo, l'attitudine predittiva del modello, nonché la logica globale dello stesso, intesa come una spiegazione semplificata e umanamente comprensibile del come input casuali producano output casuali. Per maggiore approfondimento sulle varie tipologie di spiegazioni modello-centriche e soggetto-centriche si veda L. EDWARDS e M. VEALE, Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017, 22.

[440] A.D. SELBST e J. POWLES, Meaningful Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017, 238 ss.

[441] GDPR, Considerando 71.

[442] GDPR, Considerando 60.

non danno agli utenti commerciali un ragionevole grado di prevedibilità sugli aspetti più importanti della relazione contrattuale".

La formula utilizzata dal legislatore sembrerebbe perciò suggerire che, da un lato, i requisiti di specificità e dettaglio sono strumentali alla comprensibilità del linguaggio mentre, dall'altro, il grado di dettaglio non è generalizzato all'intera pletora di informazioni, ma soltanto su quelle "questioni commerciali importanti" che sono tali nella misura in cui offrono "un ragionevole grado di prevedibilità sugli aspetti più importanti della relazione contrattuale".

Ancora una volta, quindi, il dato letterale favorisce la tesi per cui la spiegazione non deve consistere in una descrizione onnicomprensiva di tutti i parametri presi in considerazione. Il regolamento (UE) 2019/1150, tuttavia, consente di compiere un passo ulteriore, indicando qual è il criterio che il titolare deve seguire nella selezione delle informazioni e, *a contrario*, l'interessato può invocare nel richiedere chiarimenti: l'importanza ai fini della prevedibilità del processo decisionale[443].

Si può quindi concludere che una spiegazione sarà qualificabile come significativa nella misura in cui offra all'interessato informazioni relative a una selezione ragionata dei parametri presi in considerazione che, seppure non esaustiva, consente all'interessato di prevedere, con "un ragionevole grado di probabilità", l'esito del processo decisionale automatizzato e di capire come modificare il proprio comportamento per potervi influire[444].

[443] In questo senso, il regolamento (UE) 2019/1150 sembrerebbe chiarire la posizione già genericamente assunta dal Gruppo di lavoro articolo 29 nelle sue linee guida sui processi decisionali automatizzati dove, riferendosi all'articolo 22 GDPR, affermava come "il titolare del trattamento dovrebbe fornire all'interessato informazioni di carattere generale (in particolare, sui fattori presi in considerazione per il processo decisionale e sul rispettivo "peso" a livello aggregato) che sono utili all'interessato anche per contestare la decisione." GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 30.

[444] Tale conclusione sembrerebbe supportata anche dalla lettura dei lavori preparatori della normativa. In particolare, la Commissione per l'industria, la ricerca e l'energia nel suo parere aveva proposto un emendamento al considerando 17 al fine di puntualizzare la nozione di parametro principale come riferita a ogni meccanismo di aggiustamento "di importanza fondamentale per un'adeguata comprensione del funzionamento del sistema di posizionamento". Allo stesso modo, la Commissione aveva anche proposto un emendamento al considerando 18 al fine di sostituire la dicitura "parametri principali" con l'espressione "descrizione pubblicamente accessibile dei parametri di importanza fondamentale per un'adeguata comprensione del modo in cui è determinato il posizionamento." ANNA ZÁBORSKÁ, *Parere della commissione per l'industria, la ricerca e l'energia destinato alla commissione per il mercato interno e la protezione dei consumatori sulla proposta di regolamento del Parlamento europeo e del Consiglio che*

Ne consegue, inoltre, che la specificità dovrebbe impedire l'adozione di termini e condizioni generali dei propri servizi non comprensibili (*rectius* significativi). Dovrebbero quindi essere proibite descrizioni standardizzate attraverso l'utilizzo di termini vaghi. Al contrario, al titolare del trattamento è imposta la formulazione di spiegazioni costantemente aggiornate e differenziate in base alla particolare tipologia di trattamento e settore di *business* (*rectius* finalità), alle categorie di destinatari e, conseguentemente, ai parametri che consentono di rendere prevedibili gli aspetti che tale specifica categoria di destinatari reputa più importante[445].

Neanche in quest'ottica, quindi, la tesi della spiegazione controfattuale sembrerebbe conforme al dettato normativo nella misura in cui darebbe il diritto all'interessato di conoscere solo uno dei parametri presi in considerazione: quello che gli consentirebbe di ottenere l'esito desiderato apportando il più piccolo cambiamento alla sua situazione iniziale. In tal senso, la spiegazione controfattuale non appare né comprensibile né specifica. Non è comprensibile perché non mette l'interessato nella condizione di poter prevedere neanche in parte l'esito del processo decisionale. Non è specifica perché seleziona il parametro da mostrare in base a ciò che può essere modificato con il minor sforzo dall'interessato, a prescindere dal peso che questo ha esercitato sulla decisione e dell'importanza che tale aspetto riveste per l'interessato stesso. Anzi, proprio perché ispirato al c.d. "più vicino dei mondi possibili" è probabile che il parametro svelato riguardi un aspetto del tutto marginale della relazione contrattuale, con peso relativo minimo rispetto ad altri parametri, e del tutto inutile per l'interessato, che nulla può inferire da tale informazione circa il funzionamento complessivo del sistema[446].

---

promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online (PARLAMENTO EUROPEO, 23 novembre 2018), 2018/0112(COD), 14-20.

[445] Questa lettura è supportata anche dall'articolo 5 paragrafo 5 regolamento (UE) 2019/1150 in base al quale "[l]e descrizioni di cui ai paragrafi 1, 2 e 3 devono essere tali da consentire agli utenti commerciali o agli utenti titolari di un sito *web* aziendale di comprendere chiaramente se, come e in quale misura il meccanismo di posizionamento tiene conto dei seguenti elementi: a) le caratteristiche dei beni e dei servizi offerti ai consumatori tramite i servizi di intermediazione online o il motore di ricerca online; b) la *pertinenza di tali caratteristiche per i suddetti consumatori*; c) per quanto riguarda i motori di ricerca online, le caratteristiche grafiche del sito web utilizzato da utenti titolari di un sito web aziendale". Corsivo aggiunto.

[446] Tra l'altro si dovrebbe anche considerare la circostanza per cui non tutti i valori presi in considerazione dal sistema possono essere modificati. Ad esempio, è difficile pretendere che un soggetto cambi la propria etnia, la propria religione, le proprie preferenze, ma, in alcune circostanze ciò può valere anche per dati non sensibili quali il proprio reddito o la propria residenza. Ne consegue che, nel caso in cui il sistema decisionale automatizzato dovesse seguire una logica discriminatoria, perché addestrato con dati portatori di pregiudizi insiti nel campione utilizzato, sapere che cambiare il proprio reddito o la propria

In questo senso, il percorso interpretativo sin qui seguito sembrerebbe avvicinarsi maggiormente alla posizione di chi, come Selbst e Powles, ritiene controproducente imporre un contenuto standard, unico ed invariabile, alla spiegazione[447]. Molto più efficace, sostengono gli Autori, sarebbe adottare una prospettiva squisitamente funzionale, dove lo standard minimo da seguire per adempiere l'obbligo di formulazione di una spiegazione significativa viene fissato in base agli obiettivi da raggiungere: essere trasparente per l'interessato (*ex* art.5 GDPR) e facilitarne l'esercizio dei diritti (*ex* art. 12 GDPR), in particolare del diritto di contestare la decisione[448].

La tesi per cui l'introduzione dell'aggettivo *significativo* richiami l'idea di un'informazione utile, intelligibile e azionabile da parte degli interessati, peraltro, sembrerebbe condivisa anche dalla Commissione europea, la quale, nella valutazione d'impatto del nuovo regolamento (UE) 2019/1150, ha qualificato la motivazione imposta dall'articolo 4 come un "*actionable statement*"[449]. In particolare, infatti, oltre i doveri informativi già menzionati, il regolamento prevede anche che, ove un fornitore di servizi

residenza avrebbe determinato un *output* favorevole da parte del sistema non consente comunque di valutare la contestabilità della decisione in quanto discriminatoria. Ciò è vero nella misura in cui non si è messi nella condizione di poter valutare che peso ha esercitato il dato rispetto alle altre variabili e se, ad esempio nel caso della residenza, quest'ultima sia risultata un fattore rilevante in quanto *proxy* di un dato sensibile, e quindi discriminatorio, quale l'etnia o la religione. Cfr. K. BRENNAN-MARQUEZ, "Plausible Cause": Explanatory Standards in the Age of Powerful Machines, 70, *Vanderbilt Law Review*, 2017, 7; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H.YU, Accountable Algorithms, 165, *University of Pennsylvania Law Review*, 2017, 633; T. MILLER, P. HOWE, L. SONENBERG, Explainable AI: Beware of Inmates Running the Asylum Or: How I Learnt to Stop Worrying and Love the Social and Behavioural Sciences, *ArXiv*, 2017, 3. Ribadisce la difficoltà a prevenire ed individuare *output* discriminatori ROHEN, il quale sottolinea come "[a] data controller may not be aware of bias in the resulting profiling decisions because the processing of sensitive data would be required for their verification, and such processing could be unlawful. Ironically, the prohibition in Article 9(1) GDPR may therefore prevent the discovery of the resulting indirect discrimination. Discovering discriminatory effects of algorithms without direct verification is largely an unsolved problem." M. RHOEN e Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018, 151.

[447] Un *favor* verso una tecnica normativa improntata alla flessibilità è stato mostrato anche dalla Commissione per i trasporti e il turismo, la quale aveva proposto un emendamento deputato all'introduzione di un nuovo considerando 6 *ter* volto a sottolineare che "una migliore regolamentazione nell'era digitale richiede una legislazione basata su principi, accompagnata da azioni complementari non normative per un efficace adeguamento alle nuove tecnologie e ai nuovi modelli imprenditoriali, al fine di prevenire la frammentazione del mercato unico." . ȚAPARDEL, *Parere della Commissione per i trasporti e il turismo destinato alla Commissione per il mercato interno e la protezione dei consumatori sulla proposta di regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online* (PARLAMENTO EUROPEO, 23 novembre 2018) (2018/0112(COD)), 7.

[448] A.D. SELBST e J. POWLES, Meaningful Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017, 242

[449] *Commission Staff Working Document Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services* (CONSIGLIO DELL'UNIONE EUROPEA, Bruxelles 30 aprile 2018) 2018/0112 (COD), 49.

di intermediazione online decida di limitare o sospendere la fornitura dei suoi servizi di intermediazione online a un determinato utente commerciale, debba provvedere a comunicargli le motivazioni di tale decisione e predisporre un processo interno di gestione dei reclami che dia all'utente l'opportunità di chiarire i fatti e le circostanze che hanno portato alla decisione stessa. A tal fine, chiarisce inoltre il regolamento, la motivazione "dovrebbe permettere agli utenti commerciali di accertare se vi siano margini per contestare la decisione e, di conseguenza, aumentare le loro possibilità di un efficace ricorso ove necessario. L'esposizione delle motivazioni dovrebbe identificare le ragioni della decisione, *in base alle indicazioni enunciate in precedenza* dal fornitore nei termini e nelle condizioni, e fare riferimento in modo *proporzionato* alle relative circostanze […] che hanno condotto a tale decisione"[450].

Il testo del regolamento sembrerebbe perciò suggerire che l'intenzione del legislatore eurounitario sia stata quella di intensificare i doveri di *disclosure* del fornitore di servizi *online* nella fase di reclamo, imponendogli di contestualizzare le informazioni "specifiche e dettagliate" (secondo l'accezione precedentemente adottata) incluse nei termini e nelle condizioni del servizio[451]. Tale contestualizzazione, però, ancora una volta, non sembrerebbe dover essere assoluta, ma dovrebbe avvenire in modo "proporzionato" e strumentale al rafforzamento della capacità degli utenti di verificare l'esistenza e la fondatezza di eventuali motivi di reclamo.

Tale duplice e graduale grado di dettaglio degli obblighi di trasparenza disciplinato dal regolamento (UE) 2019/1150, richiama e chiarisce la differenza tra i doveri di notifica *ex ante ex* artt. 13-14 GDPR e la spiegazione *ex post* della decisione

[450] Regolamento (UE) 2019/1150 del Parlamento Europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, G.U. L 186/57, Considerando 22.

[451] L'idea di un obbligo informativo aggiuntivo rispetto a quello imposto rispetto alle condizioni e termini generali del servizio è suggerita anche dalla Commissione, la quale, in fase di adozione del regolamento, ha ribadito come l'informazione precontrattuale sui criteri utilizzati per determinare il *ranking* dei risultati ricerca online deve essere offerta ai consumatori in modo chiaro e comprensibile, non solamente nei termini e condizioni generali del servizio. *Commission Staff working document-Impact assessment accompanying the document proposals for directives of the European Parliament and of the Council amending Council Directive 93/13/EEC, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules and on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC* (COMMISSIONE EUROPEA, Bruxelles, 11 aprile 2018), SWD(2018) 96 final pt. 1/3, 45.

che, ai sensi dell'articolo 22 e del considerando 71 del GDPR, dovrebbe prendere in considerazione le circostanze e il contesto specifici del trattamento[452].

Tale differenziazione, peraltro, sembrerebbe anche placare i timori avanzati da chi sostiene che una eccessiva trasparenza, oltre che violare i segreti commerciali dei titolari, potrebbe compromettere l'efficienza stessa del sistema decisionale automatizzato nella misura in cui consentirebbe agli interessati di prevederne gli esiti con un grado di precisione tale da poterne manipolare il funzionamento[453].

Alla luce delle considerazioni sin qui svolte, una spiegazione può risultare significativa ove offra una descrizione ragionata di quei parametri utilizzati che, tenuto conto della finalità del trattamento e delle categorie di soggetti interessati, risultino essere più utili a consentire a questi ultimi di prevedere e influire sull'esito del processo

[452] In tal senso, la formulazione del regolamento (UE) 2019/1150 sembrerebbe ancora una volta condividere ed approfondire le posizioni assunte nel GDPR, così come nella Convenzione 108+. Lo stesso Consiglio d'Europa aveva sottolineato il collegamento funzionale tra la spiegazione e l'esercizio dei diritti dell'interessato, affermando che "nel caso del grado di affidabilità creditizia, [ad esempio], gli interessati dovrebbero avere il diritto di conoscere la logica alla base del trattamento dei loro dati risultante in una decisione "sì" o "no" e non semplicemente informazioni sulla decisione stessa. In assenza di comprensione di questi aspetti non potrebbe esserci alcun effettivo esercizio di altre garanzie essenziali quali il diritto di opposizione e il diritto di proporre reclami presso un'autorità competente". AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), *Explanatory Report of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) (128esima Sessione del Comitato dei Ministri, Elsinore 17-18 maggio 2018), § 77.

[453] Tale timore è espressamente statuito dall'articolo 5 paragrafo 6 Direttiva Omnibus, in base alla quale "i fornitori di servizi di intermediazione *online* e i fornitori di motori di ricerca *online*, nell'adempiere alle prescrizioni del presente articolo, non sono tenuti a rivelare algoritmi o informazioni che, con ragionevole certezza, si tradurrebbero nella possibilità di trarre in inganno i consumatori o di arrecare loro danno attraverso la manipolazione dei risultati di ricerca. Il presente articolo lascia impregiudicata la direttiva (UE) 2016/943." Così anche il considerando 27 del regolamento (UE) 2019/1150 per cui la capacità dei fornitori di servizi online "di agire contro la manipolazione in mala fede del posizionamento da parte di terzi, anche nell'interesse dei consumatori, dovrebbe ugualmente non essere compromessa. Una descrizione generale dei parametri principali di posizionamento dovrebbe salvaguardare tali interessi, fornendo nel contempo agli utenti commerciali e agli utenti titolari di siti *web* aziendali una adeguata comprensione del funzionamento del posizionamento nel contesto del loro utilizzo di servizi di intermediazione online o di motori di ricerca online specifici." Analoghi timori sono poi condivisi dal Comitato Economico e Sociale, il quale sebbene nel suo parere si sia dichiarato "favorevole alla pubblicazione da parte dei fornitori di servizi *online* dei principali parametri per il posizionamento di annunci e siti *web*", ha fatto notare che "questa iniziativa necessita di essere gestita con cautela poiché potrebbe favorire truffe da parte degli utenti commerciali a danno di altre imprese o consumatori, generando distorsioni del mercato". J. MULEWICZ e A. LONGO, *Parere del Comitato economico e sociale europeo sulla a) «Proposta di direttiva del Parlamento europeo e del Consiglio relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE»* [COM(2018) 184 final — 2018/0089 (COD)] *e sulla b) «Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 93/13/CEE del Consiglio del 5 aprile 1993, la direttiva 98/6/CE del Parlamento europeo e del Consiglio, la direttiva 2005/29/CE del Parlamento europeo e del Consiglio e la direttiva 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'UE relative alla protezione dei consumatori»* [COM(2018) 185 final — 2018/0090 (COD)], § 5.3.

decisionale automatizzato. Tale descrizione, tuttavia, non impone la divulgazione di segreti commerciali (incluso l'algoritmo[454]) e "non deve necessariamente essere fornita individualmente per ogni ricerca effettuata"[455].

Allo scopo, peraltro, il titolare è tenuto a adottare misure organizzative interne che gli consentano, in fase di reclamo, di offrire tale maggior grado di dettaglio all'interessato, contestualizzando le informazioni fornite in precedenza. In particolare, l'interessato ha il diritto di conoscere quali sono gli specifici fatti che, rientrando nelle categorie descritte nelle condizioni e termini del servizio, sono stati presi in considerazione dal sistema per addivenire alla decisione che lo riguarda individualmente. In un'ottica di bilanciamento di interessi, infine, il legislatore sembrerebbe venuto ancora una volta incontro al titolare del trattamento, consentendogli anche in questa fase di astenersi dal ricostruire l'intera fattispecie concreta, potendo selezionare tra tutte le circostanze del caso, quelle che meglio consentono all'interessato di valutare (e quindi argomentare) la fondatezza degli specifici motivi di reclamo allegati.

2.5. Proposte di spiegazione: una ricognizione esegetica

Il percorso interpretativo sin qui condotto ha consentito di ricostruire, alla luce del più recente e maturo linguaggio adottato dal legislatore europeo nel c.d. *New Deal for Consumers*, in che termini il titolare del trattamento, pur non essendo tenuto a fornire

[454] In questo senso si esprimono in modo univoco tutte le normative richiamate. La direttiva Omnibus al Considerando 23 stabilisce che "l'obbligo di informazione in merito ai principali parametri che determinano la classificazione non pregiudica le disposizioni della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio. I professionisti non dovrebbero essere obbligati a comunicare il funzionamento dettagliato dei loro meccanismi di classificazione, compresi gli algoritmi." Nello stesso senso si esprime il regolamento (UE) 2019/1150 che al considerando 27 stabilisce che "Ai fornitori di servizi di intermediazione online o di motori di ricerca online non dovrebbe essere richiesto di divulgare il funzionamento dettagliato dei loro meccanismi di posizionamento, inclusi gli algoritmi, a norma del presente regolamento. […] A tale riguardo, mentre il presente regolamento non pregiudica la direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, la descrizione data dovrebbe perlomeno essere basata sui dati effettivi relativi alla rilevanza dei parametri di posizionamento utilizzati." Ancora, in senso analogo si è espressa la Commissione giuridica affermando che "per quanto riguarda la trasparenza in materia di posizionamento, il relatore ritiene che sia necessario trovare un equilibrio rispetto alle norme sulla concorrenza. Dovrebbero quindi essere necessarie piattaforme per divulgare i principi alla base dei parametri che determinano il posizionamento, ma non gli algoritmi stessi, che dovrebbero essere considerati segreti commerciali." F. ZAMMIT DIMECH, *Parere della commissione giuridica destinato alla commissione per il mercato interno e la protezione dei consumatori sulla proposta di regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online* (Parlamento europeo, 26 novembre 2018) - COM(2018)0238, 3.

[455] Direttiva Omnibus, Considerando 23.

"una spiegazione di una particolare decisione"[456], debba comunque rispettare il diritto dell'interessato ad ottenere "informazioni sulla logica effettivamente utilizzata, e non solamente relative al generale funzionamento di sistema di un processo decisionale algoritmico"[457].

Superato così l'*empasse* interpretativo concernente il contenuto teorico della spiegazione, si procederà ad analizzare in che modo, e sino a che punto, tale quadro normativo sia effettivamente ed efficacemente implementabile.

Se si muove dall'assunto per cui, come si è tentato di dimostrare, la spiegazione deve essere: (i) significativa nel senso di quantitativamente ragionata; (ii) specifica nel senso di diversificata in base alla finalità del trattamento e alle categorie di interessati; e (iii) suscettibile di essere proporzionalmente contestualizzata in fase di reclamo; si può osservare una graduazione dei doveri di motivazione del titolare del trattamento tale per cui l'obbligo di informazione preventiva concernente il processo decisionale automatizzato sembrerebbe potersi assestare su un grado di personalizzazione che, pur dovendo trascendere la standardizzazione, non arriva all'individualità. Al contrario, ove la decisione automatizzata sfoci in una fase di reclamo, il titolare del trattamento sarà obbligato a superare la dimensione collettiva e calare la logica algoritmica nelle specifiche circostanze del caso concreto.

2.5.1. La spiegazione ante-reclamo: una prospettiva di "gruppo"

Iniziando la ricostruzione degli ostacoli all'assolvimento di tale obbligo rispetto alla fase pre-reclamo, si deve innanzitutto osservare che se la descrizione del processo decisionale automatizzato non può essere completamente standardizzata, ma non deve essere necessariamente individualizzata, rimane un unico livello intermedio di personalizzazione che è quella improntato alla dimensione del gruppo.

Come correttamente affermato, sebbene la *data analytics* possa oggi condurre all'adozione di decisioni pericolose a livello aggregato per gruppi di persone, la

[456] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 30.

[457] G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 256.

concettualizzazione giuridica nella nozione di privacy non è mai andata oltre quella di una pluralità di individui collettivamente portatori di diritti individuali[458].

Storicamente i gruppi sono riguardati come composti da una moltitudine di persone fisiche individuate sulla base di comunanze percepite dagli stessi membri oppure dall'esterno, ma pur sempre rilevabili a livello umano attraverso un processo di raggruppamento del quale i soggetti interessati sono pienamente consapevoli: perché dagli stessi avviato o perché dagli stessi conoscibile[459]. Oggi, al contrario, le correlazioni rilevate con sistemi di *machine learning* rappresentano un nuovo strumento di raggruppamento, potente al punto che "[*g*]*roups can now seem to automatically present themselves within data, even as the picture of the individual members remains fuzzy. Big Data thus changes what a group is and, in the same sweep, what an individual is*"[460].

Peraltro, la definizione di gruppi può avvenire in modo "controllato", come nel caso in cui il titolare si avvalga di forme supervisionate di ML e quindi predetermini le caratteristiche che i membri del gruppo devono presentare, ma sempre più spesso avviene in modo "spontaneo". Ciò avviene, ad esempio, ogni qualvolta il titolare scelga di

[458] Nelle parole degli Autori "[*t*]*he search for group privacy can be explained in part by the fact that with Big Data analyses, the particular and the individual is no longer central. In these types of processes, data is no longer gathered about one specific individual or a small group of people, but rather about large and undefined groups. Data is analysed on the basis of patterns and group profiles; the results are often used for general policies and applied on a large scale*." L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT, *Introduction: A New Perspective on Privacy*, in ID. (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 1-5. Cfr, ALESSANDRO MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 140, il quale sottolinea come "[*n*]*either the notion of decisional privacy nor its constitutional dimension, originating in the ground-breaking opinion given by Brandeis in his role as Supreme Court judge, abandoned the individualistic nature of the right*." Cfr. *Olmstead v. United States*, 277 U.S. 438, 471 (1928).

[459] Il concetto è autorevolmente espresso da MANTELERO: "*Nowadays, new technologies and powerful analytics make it possible to collect and analyse huge amounts of data. In many cases, the general purposes of this new concentration of control over information no longer concern single persons, but adopt a large-scale perspective. Analytics investigate attitudes and behaviour of large groups, communities, and even entire countries. Moreover, these new forms of analysis do not necessarily investigate pre-existing groups. Groups are created by data gatherers selecting specific clusters of information. Data gatherers shape the population they set out to investigate and collect information about different people who do not know the other members of the group and, in many cases, are not aware of the consequences of their belonging to a group*." A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 145.

[460] LANAH KAMMOURIEH, THOMAS BAAR, JOS BERENS, EMMANUEL LETOUZÉ, JULIA MANSKE, JOHN PALMER, DAVID SANGOKOYA, e PATRICK VINCK, *Group Privacy in the Age of Big Data*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 40 ss.

utilizzare forme non supervisionate di ML, rimettendo interamente all'algoritmo il processo di raggruppamento che rimane quindi inconoscibile allo stesso programmatore. In quest'ultimo caso, quindi, i gruppi rimangono latenti ed imperscrutabili tanto dai suoi membri quanto dal titolare[461].

Ne consegue che, l'utilizzo del ML non supervisionato a fini decisionali, nella misura in cui non consente al titolare di individuare i parametri utilizzati e il peso relativo ad essi assegnato dal sistema nell'addivenire alla determinazione automatizzata, non può essere compatibile con il quadro normativo così come ricostruito nel precedente paragrafo[462]. Meno chiara, ma comunque problematica, è l'ammissibilità di decisioni prodotte da sistemi di ML supervisionato rispetto alle quali sarebbe senz'altro più agevole risalire ai parametri utilizzati, ma che rendono comunque complessa la ricostruzione della logica interna seguita del sistema e, conseguentemente, del peso esercitato dalle varie variabili [463].

---

[461] Lanah Kammourieh *et al.* denunciano questa opacità ammonendo circa i suoi rischi. In particolare, gli autori sottolineano come "[*t*]*his incomplete awareness of how and on which grounds group identification takes place could lead to an epistemic dependence on processes we might no longer fully understand*". ID., *Group Privacy in the Age of Big Data,* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 43.

[462] Sull'insufficienza del livello di *esplicability* offerto dalle attuali tecniche disponibili per ricostruire la logica seguita dai sistemi di ML, si veda quanto argomentato in C. TABARRINI, Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019, 555 ss, spec. nt. 76. In particolare, si ricorda che "Il metodo LOCO ("*Leave One Column Out*"), consiste nell'eliminare una variabile alla volta, ricalcolando poi il risultato. Maggiore sarà la variazione di questo nuovo esito rispetto a quello iniziale, maggiore sarà il peso esercitato dalla variabile eliminata sulla decisione automatizzata. Analogamente, il metodo PI (P*ermutation impact*) implica la sostituzione di una variabile con una diversa e casuale, ricalcolando poi il risultato. Infine, il metodo LIME ("*Local Interpretable Model-Agnostic Explanations*") utilizza un'approssimazione lineare del modello per tradurre in termini più semplici il funzionamento reale del modello, avvalendosi peraltro di variabili sintetiche. In altri termini si tratta di una simulazione semplificata con dati fittizi del modello reale." Cfr. J. BUDZIK, *Most AI Explainability is Snake Oil. Ours isn't* (ZestFinance, 2019) disponibile all'indirizzo *https://www.zestfinance.com/snake-oil-explainability*.

[463] Per una panoramica dei più recenti sviluppi nel campo dell'Intelligenza Artificiale si veda G.F. ITALIANO, *Intelligenza Artificiale: passato, presente e futuro*, in F. PIZZETTI (a cura di), *Intelligenza Artificiale, Protezione dei Dati Personali e Regolazione*, G. Giappichelli Editore, Torino, 2018, 216 ss. Più nello specifico, autorevoli e pionieristiche riflessioni sul tema dell'opacità dei sistemi di IA sono state avanzate da Jenna Burrell la quale ha evidenziato tre livelli di opacità di tali tecnologie "(1) *opacity as intentional corporate or institutional self-protection and concealment and, along with it, the possibility for knowing deception*; (2) *opacity stemming from the current state of affairs where writing (and reading) code is a specialist skill and*; (3) *an opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of semantic interpretation*." JENNA BURRELL, How the machine 'thinks': Understanding opacity in machine learning algorithms, 1, *Big Data & Society*, 2016, 1-2. Cfr. B. LEPRI, J. STAIANO, D. SANGOKOYA, E. LETOUZÉ, e NURIA OLIVER, The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, Studies in *Big Data*, Vol. 11, Berlino, Springer, 2017, 12 ss. Sull'impossibilità tecnologica di risalire alla logica algoritmica interna di gran parte dei sistemi di ML

Una spiegazione ante-reclamo potrebbe assumere la seguente formulazione: "Il premio della polizza auto è determinato sulla base di una molteplicità di parametri, tra cui l'età del guidatore, il modello del veicolo, lo storico dei sinistri in cui l'assicurato è stato coinvolto, l'area geografica di residenza e la professione. Per i guidatori che rientrano nella fascia di età B-C, di regola, l'età è il fattore che maggiormente pesa sul premio della polizza, incidendovi per il X%, seguito dalla professione, che incide per lo Y%, e dall'area geografica che incide per Z%. Per i guidatori nella fascia di età A-B, invece, la professione e la collocazione geografica sono i parametri che più pesano sull'ammontare del premio, ammontando entrambi allo V% dello stesso. Se però l'assicurato vive nella zona geografica G, il premio salirà dello P% a prescindere dall'età."

In tal modo si rispetterebbe il quadro normativo, così come ricostruito nel precedente paragrafo, nella misura in cui: (i) vengono indicati i principali parametri utilizzati nel prendere la decisione; (ii) viene specificato il peso relativo esercitato dagli stessi; (iii) la selezione e descrizione del peso dei parametri non è standardizzata, ma parametrata alle diverse categorie di clienti, indicando per ciascuna i parametri che esercitano maggior peso e quindi sono più rilevanti per comprendere ed eventualmente contestare la decisione.

Pur ammettendo la discussa (e discutibile) fattibilità computazionale di una tale spiegazione, rimane da verificare se e in che misura sia giuridicamente, prima ancora che tecnologicamente, possibile per il titolare contestualizzare una tale descrizione in fase di reclamo.

2.5.2. La spiegazione post-reclamo: l'accesso al profilo

Riepilogando le conclusioni fin qui raggiunte, ai sensi dell'articolo 15 GDPR, l'interessato ha il diritto di accedere a tutti i suoi dati personali detenuti e trattati dal titolare. In tal modo, potrà senz'altro verificare se la decisione si fonda su informazioni errate, ovvero discriminatorie[464].

attualmente utilizzato, si vedano le osservazioni compiute in C. TABARRINI, Comprendere la "*Big Mind*": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019, 555 ss.

[464] Sull'esigenza di implementare strumenti efficaci di controllo e prevenzione di forme di discriminazione algoritmica si vedano le parole del RAPPORTEUR J.P. ALBRECHT, per il quale "[*p*]*rofiling*

Ove nessuna di queste censure possa essere mossa, all'interessato non rimane che richiedere l'intervento di un operatore umano, al fine di poter contestare la decisione e ottenerne una rivalutazione non automatizzata. A tal fine, avrà diritto ad avere informazioni "significative" sulla logica algoritmica che, come già osservato, in questa fase di reclamo saranno tali se prendono in considerazione il contesto e le circostanze specifiche in cui è avvenuto il trattamento e danno all'interessato la possibilità di chiarire i fatti e le circostanze alla base della decisione[465].

Riprendendo l'esempio fornito in precedenza, si potrebbe immaginare che l'assicurato non contesti la correttezza delle informazioni utilizzate, né possa lamentarne il carattere discriminatorio, ma ritenga che le inferenze che il sistema ha estrapolato da tali dati non siano rappresentative. In altri termini, ciò che l'interessato vuole contestare è quello specifico "fatto" su cui è basata la decisione che nel contesto *Big Data* è costituito dal profilo[466].

Il profilo può essere definito come quel frammento dell'identità del soggetto interessato, rilevante per lo specifico settore di mercato[467], che viene inferito in modo automatizzato non tanto dal complesso di dati personali dell'interessato stesso, ma dalle comunanze che questi mostrano con i dati relativi ad una collettività indeterminata di

that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9." ID., *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Committee on Civil Liberties, Justice and Home Affairs, 21 novembre 2013), 94. Cfr. F. DI RESTA, *La nuova 'Privacy europea': i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore, Torino, 2018, 52-54.

[465] Si veda la ricostruzione del quadro normativo di riferimento compiuta *supra* § 2.4.

[466] Sulla tendenza a convertire dati personali in cc.dd. "*quantified selves*" si vedano le interessanti riflessioni di A. DEMBOSKY, *Invasion of the Body Hackers* (Financial Times, 10 giugno 2011). Cfr. N. DOW SCHÜLL, Self in the Loop: Bits, Patterns, and Pathways in the Quantified Self, in Z. PAPACHARISSI (a cura di), *A Networked Self and Human Augmentics, Artificial Intelligence, Sentience*, Routledge, New York, 2019, 26-30; F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015, 2 spec. nt. 5. Cfr. D. KEATS CITRON e F. PASQUALE, The Scored Society: Due Process for Automated Predictions, 89, *Washington Law Review*, 2014, 1, 10ss

[467] Per una esemplificazione delle possibili applicazioni della profilazione per cluster nel settore bancario-finanziario a fini di Custom Relation Management, valutazione del merito creditizio e consulenza finanziaria, si veda R. FRAU, *Il trattamento dei dati personali nell'attività bancaria*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 664-665.

soggetti[468]. È, sostanzialmente, dall'analisi del comportamento dei soggetti che presentano tratti affini all'interessato, che le tecniche di *data analytics* consentono di trarre inferenze sulla personalità dell'interessato, prevedendone (nonché influenzandone) azioni e scelte[469]. Non è peraltro la tecnica in sé a creare problemi, alla base di ogni indagine statistica, ma il grado di dettaglio e precisione con cui si possono misurare aspetti della personalità in alcun modo quantificabili al di fuori di un contesto *Big Data*[470].

Ci si chiede quindi se l'interessato abbia diritto, quantomeno in fase di reclamo, ad accedere al suo profilo, inteso come quella serie di caratteristiche che gli sono artificialmente attribuite quali presunti tratti della sua personalità e sulla base dei quali è stata assunta la decisione contestata. Ciò risulta fondamentale nella misura in cui nel contesto *Big Data* il profilo è l'espressione più pura della logica algoritmica e condensa il prodotto di tutte le inferenze rilevate che hanno preceduto e influenzato la scelta delle variabili e il peso ad esse attribuito. Ove l'interessato non possa contestare che vive in una determinata area geografica, perché rispondente al vero, può conoscere (e quindi contestare) l'inferenza che da quel dato è stata tratta su di lui per prendere la decisione nei suoi confronti?

Il Consiglio d'Europa sembrerebbe aver dato una risposta positiva al quesito, riconoscendo all'interessato il diritto di poter argomentare "*the irrelevance of the profile*

[468] Sull'arricchimento dati per aggregazione si vedano, *ex multis*, le riflessioni di R. DE MEO, Autodeterminazione e consenso nella profilazione dei dati personali, *Dir. Inf.*, 2013, 587 ss.

[469] Circa il timore che la capacità dei singoli di influire sulle decisioni che li riguardano venga offuscata dalla propria "ombra informativa" riecheggia l'attualità dei lungimiranti timori avanzati dalla Commissione Europea e dal Consiglio d'Europa, il quale oltre un decennio fa ricordava come già nel 1990 la prima avesse ammonito sul rischio che "[*t*]*he use of extensive data profiles of individuals by powerful public and private institution deprives the individual the capacity to influence decision-making processes within those institutions, should decisions be taken on the sole basis of his 'data shadow'*". Così COMMISSIONE EUROPEA, *Commission communication on the protection of individuals in relation to the processing of personal data*, COM(90) 314 fin. SYN 287, Bruxelles, 13 settembre 1990, 29, citato da, J.M. DINANT, C. LAZARO, Y. POULLET, N. LEFEVER e A. ROUVROY, *Application of Convention 108 to the Profiling Mechanism Some Ideas for the Future Work of the Consultative Committee* (CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, Strasburgo, 11 gennaio 2008), 13.

[470] GENEVA ASSOCIATION, *Big Data and Insurance: Implications for Innovation, Competition and Privacy*, Zurigo, 2018, 22ss. In senso analogo si è recentemente espressa A. PIERUCCI, la quale sottolinea come "la particolarità della profilazione è che la collocazione della persona in una o l'altra categoria si svolge attraverso criteri determinati da terzi, spesso fondati su matrici probabilistiche che, non tenendo conto delle molte variabili che ruotano intorno alla persona, potrebbero portare all'adozione di decisioni sintetiche che non corrispondono alle sue effettive condizioni e/o che generano forme di discriminazione, o di esclusione a beni o servizi." ID., *Elaborazione dei dati e profilazione delle persone*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., 416. Cfr. B.W. SCHERMER, The Limits of Privacy in Automated Profiling and Data Mining, 27, *Computer Law & Security Review*, 1, 2011, 45ss.

to be applied to his or her particular situation, of other factors that will have an impact on the result of the automated decision"[471].

Al contrario, tuttavia, si potrebbe obiettare che i profili, in quanto metadati inferiti da una massa anonimizzata di dati personali e riferibili ad un gruppo di interessati complessivamente considerati, esulano dallo scopo di applicazione del GDPR, così come definito dall'articolo 2 paragrafo 1 in combinato disposto con l'articolo 4 paragrafo 1[472]. Nel corso del processo di *data analytics*, infatti, i dati personali sono spesso anonimizzati ed aggregati in modo tale che la conoscenza offerta dai metadati ottenuti dai *pattern* fra essi rilevati trascenda la dimensione individuale e diventi altro rispetto ai singoli dati isolatamente considerati[473].

Il rilievo è però agevolmente superabile sulla scorta di una duplice serie di contro argomentazioni.

In primo luogo, sebbene il singolo interessato spesso non mostri un interesse significativo a negare il consenso al trattamento dei propri dati personali singolarmente considerati[474], ove consapevole, potrebbe invece avere maggiore interesse a non essere associato al *cluster* di individui ricostruito attraverso tecniche di *Big Data analytics* a

[471] AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), *Explanatory Report of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) (128esima Sessione del Comitato dei Ministri, Elsinore 17-18 maggio 2018), § 75.

[472] Condividono la tesi per cui al trattamento di *dataset* anonimizzati in partenza non possono trovare applicazione le tutele del GDPR M. RHOEN e Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018, 153.

[473] Una simile logica è rinvenibile nel dettato dell'articolo 4 paragrafo 10 Dir. 2019/2161/UE che, modificando l'articolo 13 direttiva 2011/83/UE, impone al professionista di astenersi "dall'utilizzare qualsiasi contenuto, diverso dai dati personali, che sia stato fornito o creato dal consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dal professionista, a meno che tale contenuto: […] c) *sia stato aggregato dal professionista ad altri dati e non possa essere disaggregato o possa esserlo soltanto con sforzi sproporzionati*" [corsivo aggiunto]. Allo stesso modo, come noto, il GDPR al considerando 26 chiarisce che "[p]er 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. 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. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

[474] Sul concetto del c.d. "*privacy paradox*" v. M. RHOEN e Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018, 157, ove viene cittoa B. SCHNEIER, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* , I ed., New York, W.W. Norton & Company, 2015, 227; D.J. SOLOVE, I've Got Nothing to Hide' and Other Misunderstandings of Privacy, 44, *San Diego L. Rev*., 2007, 745.

partire (anche) da tali dati[475]. Ciò potrebbe accadere, tornando al nostro esempio, nel caso in cui un interessato veda lievitare il premio della propria polizza a causa dell'elevata rischiosità rilevata dall'analisi aggregata dello stile di guida dei residenti nel suo stesso quartiere. In questo senso, un'analisi accurata a livello aggregato potrebbe rivelare correlazioni meramente spurie e probabilistiche a livello individuale, assegnando all'interessato profili non pertinenti alla sua condizione individuale e potenzialmente discriminatorie[476].

Una specifica declinazione di questo rischio è ben descritta da Rhoen, il quale ha sottolineato come, in un contesto *Big Data*, l'analisi di dati non sensibili possa comunque rivelare inferenze riconducibili ad aspetti della personalità degli interessati qualificabili come sensibili[477]. In particolare, l'Autore ha efficacemente descritto come i sistemi di ML, al pari di ogni sistema complesso, siano idonei a rivelare delle cc.dd. proprietà emergenti dei dati, intese come correlazioni non prevedibili dalle caratteristiche degli elementi di base del sistema. Di conseguenza, ove il sistema di ML venga addestrato utilizzando dati che, seppure apparentemente oggettivi, sono portatori di pregiudizi, il

[475] A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 146-147. Cfr. A.H. VEDDER, *Privatization, information technology and privacy: Reconsidering the social responsibilities of private organizations*, in G. MOORE (a cura di), *Business ethics: Principles and practice*, Warwick, Business Education Publishers, 1997, 215ss.

[476] In quest'ottica, non si può che condividere la posizione di chi ha sottolineato come "[*t*]*he source of concern is not the lack of secrecy and intimacy, which represents the object of group privacy, but the unfair and harmful use of data that is processed by using modern analytics*". A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 148.

[477] In questo senso si è espresso anche il Consiglio d'Europa che, nel report esplicativo della Convenzione 108, ha ribadito come "*in the era of datafication, it may be unavoidable that large data sets will contain patterns coinciding with sensitive traits because they cover 'activities resulting from (protected) opinions or beliefs'*." AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA), *Explanatory Report of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108) (128esima Sessione del Comitato dei Ministri, Elsinore 17-18 maggio 2018), § 44. Da notare, peraltro, che, come autorevolmente sostenuto, allo stato attuale la dottrina maggioritaria ritiene che l'articolo 9 para 1 GDPR non proibisce trattamenti di dati non sensibili suscettibili di rivelare informazioni qualificabili come dati sensibili. Conclusioni diverse potrebbero essere supportate dal linguaggio utilizzato dalla versione francese dell'articolo 9 para 1, mentre in senso opposto si pone la versione tedesca. Lo stesso vale per il considerando 51 GDPR che chiaramente lega il concetto di sensibilità ai dati e non alle modalità del trattamento. M. RHOEN e Q. YI FENG, Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018, 149.

sistema sarà in grado di rilevare tali correlazioni discriminatorie corrompendo l'*output* che sarà quindi viziato[478].

In secondo luogo, nel contesto *Big Data* l'efficacia delle tecniche di anonimizzazione è in constante declino a causa della sempre più ampia sfera di influenza dei dati (i.e. numero di descrittori legati a ciascun dato) e della varietà senza precedenti di patrimoni informativi con cui poterne incrociare l'analisi[479]. Ciò rende il processo di de-anonimizzazione progressivamente più agevole e meno costoso[480]. Peraltro, pur ignorando il carattere sempre più illusorio di tale tecnica di protezione dei dati personali, la *data economy* porta in sé un intrinseco *trade off* tra anonimizzazione e utilità (*rectius* valore economico) dei dati: tanto più "rumore" è inserito nel patrimonio informativo, tante meno saranno le conoscenze che dallo stesso potranno essere inferite[481].

In questo contesto è stato quindi acutamente osservato come l'anonimizzazione sia non soltanto inattuabile ma neppure auspicabile, promuovendo una nozione di privacy "sferica" (anche detta *contextual privacy*[482]) per la quale ciò che merita protezione non

[478] L'Autore rafforza la propria condivisibile posizione portando l'esempio della procedura automatizzata per le ammissioni alla St. George's Hospital Medical School. In questo caso l'algoritmo era stato addestrato con dati relativi alle precedenti ammissioni dove gli errori grammaticali erano stati valutato come un fattore negativo. A partire da tale *input*, il sistema ha inferito che fattori quali cognome e luogo di nascita erano idonei a rivelare la probabile presenza di errori grammaticali. Il risultato è stato che il numero di studenti ammessi con cognomi di origine straniera o con luogo di nascita fuori del territorio nazionale venne drasticamente ridotto. IVI, 142-143 e 150. Cfr. C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Broadway Books, 2016, 115–117; TOON CALDERS e INDRĖ ŽLIOBAITĖ, *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society*. *Data Mining and Profiling in Large Databases*, Springer, New York, 2013, 50ss.

[479] Proprio al fine di contrastare tale fenomeno in dottrina si è proposta l'introduzione di limiti normativi all'analisi incrociata, vietando l'utilizzo combinato di patrimoni informativi che, se aggregati, sono in grado di rivelare informazioni riconducibili a categorie di dati sensibili. L. KAMMOURIEH, T. BAAR, J. BERENS, E. LETOUZÉ, J. MANSKE, J. PALMER, D. SANGOKOYA, e P. VINCK, *Group Privacy in the Age of Big Data*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 50. Cfr. S. SENEVIRATNE *et al*., Predicting User Traits from a Snapshot of Apps Installed on a Smartphone, 18, *Mobile Computing and Communications Review*, 1, 2015, 6.

[480] Come rilevato dal Gruppo di Lavoro articolo 29, i rischi più frequenti sono quelli di *singling out*, *linkability* e *inferences*. Fra questi, il primo è l'unico totalmente eliminabile e soltanto attraverso l'utilizzo di due delle sette tecniche di anonimizzazione analizzate dal Gruppo. GRUPPO DI LAVORO ARTICOLO 29, *Opinion 05/2014 on Anonymisation Techniques* (Adottate il 10 aprile 2014) 0829/14/EN, WP216, 11–12. Cfr. P. OHM, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57, *UCLE Law Review*, 2010, 1701.

[481] Cfr. I.N. COFONE, *Privacy Tradeoffs in Information Technology Law*, Erasmus University, 2015, 98ss; S. MASCETTI, A, MONREALE, A. RICCI, e A. GERINO, *Anonymity: A Comparison Between the Legal and Computer Science Perspectives*, in S. GUTWIRTH, L. LEENES, P. DE HERT, Y. POULLET (a cura di), *European Data Protection: Coming of Age*, Dordrecht, Springer, 2013, 95 ss.

[482] Cfr. H. NISSENBAUM, Privacy as Contextual Integrity, 79, Washington Law Review, 1, 2004, 119ss.

sono i "*raw data*" in sé considerati, ma i metadata intesi come "*the valuable information that can be inferred from datasets*"[483]. La c.d. "*god's eye view*" offerta dai *Big Data*, infatti, si fonda su una base di dati personali talmente onnicomprensiva che, per quanto anonimizzata e aggregata, finisce sempre per offrire una conoscenza che è in qualche misura il riflesso dei comportamenti dei singoli utenti. È proprio questa, peraltro, la proprietà che rende i profili rilevanti a fini decisionali e, *a fortiori*, parte integrante di una spiegazione realmente significativa[484].

Per far fronte al problema, lungimirante dottrina ha sviluppato la nozione di "privacy collettiva" intesa come "una nuova dimensione della privacy, che ha le sue radici nella privacy individuale e condivide alcune affinità con la privacy di gruppo, ma si differenzia da entrambe"[485]. La possibilità di trarre inferenze da una quantità senza precedenti di dati, infatti, pur offrendo una forma di conoscenza che inevitabilmente trascende la dimensione individuale non implica la formazione di entità sovra-individuali giuridicamente o socialmente rilevanti. Come acutamente osservato, infatti, ogni titolare del trattamento nell'impartire al sistema automatizzato gli obiettivi di business da perseguire, finisce per isolare di volta in volta la porzione di clientela rilevante allo scopo senza che i singoli interessati coinvolti abbiano cognizione del raggruppamento o dell'identità degli altri membri. In questo processo di impercettibile "clusterizzazione" dei soggetti interessati, quindi, trovano scarsa applicazione le tradizionali nozioni di privacy di gruppo come segretezza delle informazioni condivise all'interno di una comunità (ad esempio fra soci di un'associazione o fra coniugi) ovvero come autonomia e segretezza dell'attività svolta[486].

---

[483] L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT, *Introduction: A New Perspective on Privacy*, in ID. (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 3.

[484] IBID. Cfr. D. GREENWOOD, A. STOPCZYNSKI, B. SWEATT, T. HARDJONO e A. PENTLAND, *The New Deal on Data*, in T. HARDJONO, D.L. SHRIER, A.PENTLAND (a cura di), *Trusted Data. A New Framework for Identity and Data Sharing*, MIT Press, 150 ss; M. HILDEBRANDT, Location Data, *Purpose Binding and Contextual Integrity: What's the Message?*, in L. FLORIDI (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, Vol. 17, Law, Governance and Technology Series, Springer, Cham, 2014, 31ss.

[485] In particolare, l'Autore la definisce come "*the right to limit the potential harms to the group itself that can derive from invasive and discriminatory data processing*". A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 148 e 154.

[486] Prendendo in prestito le parole di Alessandro Mantelero: "[*w*]*e are neither in the presence of forms of analysis that involve only single individuals, nor in the presence of groups in the traditional sociological meaning of the term, given the members' lack of awareness of themselves as part of a group*

Peraltro, anche nel caso in cui si volesse ammettere che i profili, in quanto metadati riferibili al gruppo anonimizzato complessivamente considerato e non al singolo a cui le caratteristiche (collettive e inferite) sono attribuite, la natura fiduciaria del rapporto che il titolare del trattamento viene ad intrattenere con il soggetto interessato (per effetto del verificarsi di una delle basi giuridiche di cui agli artt. 6 e 9 GDPR) rende il diniego di accesso al profilo incompatibile con quel dovere di cura che da tale relazione negoziale scaturisce. Come argomentato nel primo capitolo[487], infatti, se si inquadra la posizione giuridica del titolare e dell'interessato dal punto di vista del rapporto e non dell'oggetto del trattamento[488], la relazione fiduciaria che lega il titolare del trattamento al soggetto interessato non si spezza per il solo effetto della processazione del dato, perlomeno fintanto che lo stesso, per quanto rielaborato e clusterizzato, continui ad esprimere valori non solo sono riferiti all'interessato ma utilizzati per prendere decisioni automatizzate nei suoi confronti. In altri termini, nel contesto *Big Data* il dovere di cura (composto dagli obblighi posti in capo al titolare dal GDPR[489]) permane anche nella dimensione collettiva del trattamento e anche rispetto ad informazioni che non sono direttamente fornite dall'interessato, ma prodotto artificiale dell'attività di elaborazione posta in essere dal titolare e al primo riferibili per associazione algoritmica[490].

A dispetto dell'evidente stato embrionale di tali riflessioni, e pur ammettendo la possibilità di attrarre i metadati (specialmente i profili) nell'orbita di tutela garantita dal GDPR, rimangono almeno un altro ordine di ostacoli giuridici e tecnologici ad una loro effettiva *disclosure ex* art. 22 GDPR.

---

and the lack of interactions among people grouped into various categories by data gatherers". A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017, 145.

[487] Vedi meglio *supra sub* §1.6.

[488] Cfr. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, cit., 19-20; J.M. BALKIN, Information Fiduciaries and the First Amendment, 49, *U.C. Davis Law Review*, 2016, 1183, 1207, 1209; D.A. DEMOTT, Beyond Metaphor: An Analysis of Fiduciary Obligation, *Duke LJ*, 1988, 879, 882.

[489] Cfr. J.M. BALKIN, Information Fiduciaries and the First Amendment, cit., 1219-1220.

[490] Cfr. A. MANTELERO, *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, cit., 145; . B. LEPRI, J. STAIANO, D. SANGOKOYA, E. LETOUZÉ, e NURIA OLIVER, The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, cit., 2017, 12 ss.

Da un punto di vista informatico, la c.d. *cluster analysis* è un tipico problema di *machine learning* non supervisionato[491]. Di conseguenza, pur trascurando eventuali barriere normative, è tecnologicamente impossibile per il programmatore risalire ai parametri e al peso ad essi attribuito nel corso del processo decisionale, potendo soltanto valutare l'opportunità di avvalersi dell'*output*, in questo caso il profilo/gruppo di soggetti rispetto ai quali verranno adottate misure analoghe[492].

In prospettiva giuridica, invece, pur immaginando un futuro di IA in grado di risolvere problemi complessi in modo trasparente (quantomeno per i programmatori stessi), rimane da verificare se il diritto a vedere spiegata (*rectius* contestualizzata) la decisione automatizzata possa penetrare i vari strati di proprietà intellettuale che si frappongono fra l'interessato e la piena (o quantomeno efficace) *disclosure* del funzionamento del sistema di ML utilizzato.

2.6. Una spiegazione al di là della proprietà intellettuale

Guardando alla struttura del software di IA, la componente astrattamente più idonea a rivelare la logica e le idee alla base del suo funzionamento è senz'altro il codice sorgente, ovvero la serie di regole che il sistema deve rispettare per eseguire una data funzione, scritte in un linguaggio di programmazione comprensibile per gli altri programmatori, ma non leggibile dalla macchina. Per poter essere eseguiti dalla macchina, infatti, tali comandi devono essere tradotti in forma binaria, generalmente attraverso l'ausilio di un apposito programma informatico detto compilatore. Questa

[491] C. HENNIG e M. MEILA, *Cluster Analysis: An Overview*, in C. HENNIG, M. MEILA, F. MURTAGH, R. ROCCI (a cura di), *Handbook of Cluster Analysis*, NW, CRC Press-Taylor & Francis Group, 2016, 2016, 3ss. Per maggiori riferimenti circa le difficoltà tecniche che attualmente impediscono una piena ed effettiva apertura della *black box* dei sistemi di ML, specialmente se non supervisionato, si veda meglio *supra*, spec. nt. 247.

[492] Cfr. N. BAIRD, *Retail Has Three Big AI Dilemmas* (Forbes, August 13th 2018) disponibile all'indirizzo www.forbes.com/sites/nikkibaird/2018/08/13/retail-has-three-big-ai-dilemma; D. KEATS CITROW, Technological Due Process, 85, *Wash UL Rev*, 2008, 1256; K. CRAWFORD e J.SCHULZ, *Big Data* and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55, *Boston College Law Rev*, 93, 2014, 119; K. DE VRIES e M. HILDEBRANDT, Introducing Privacy, Due Process and the Computational Turn at a Glance: Pointer for the Hurried Reader, in ID. (a cura di), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, New York, 2013, 9.

nuova formulazione delle informazioni contenute nel codice sorgente è detta codice oggetto[493].

Ciò posto, è necessario chiedersi se e in che misura l'interessato abbia il diritto di ottenere l'accesso al codice sorgente, in quanto espressione della logica algoritmica che ha portato alla decisione automatizzata. Come noto, l'articolo 1 paragrafo 1 dir. 2009/24/CE riconosce tutela ai programmi per elaboratore mediante diritto d'autore. In conformità a tale disciplina, quindi, la protezione viene accordata alla forma di espressione del programma (incluso il materiale preparatorio per la sua progettazione), ove originale in quanto frutto della creazione intellettuale dell'autore, lasciando invece impregiudicato l'accesso alle idee e ai principi alla base dello stesso.

Il considerando 11 dir. 2009/24/CE chiarisce inoltre che "le idee e i principi che sono alla base della logica, degli algoritmi e dei linguaggi di programmazione non sono tutelati a norma della presente direttiva". Da tale formulazione, sembrerebbe potersi agevolmente dedurre come, in quanto *traduzione* in linguaggio di programmazione degli algoritmi alla base delle funzioni da eseguire, il codice sorgente e il codice oggetto rientrino nello scopo di applicazione della disciplina, ammontando a espressione computazionale delle idee dell'autore del programma[494].

Come osservato in dottrina, tale conclusione è poi ulteriormente confermata dall'articolo 10 paragrafo 1 dell'Accordo TRIPs, in virtù del quale i programmi per elaboratore devono essere protetti come opere letterarie ai sensi della Convenzione di Berna "*whether in source or object code*"[495].

---

[493] "*Source code* […] *is the uncompiled, non-executable code of a computer program stored in source files. It is a set of human readable computer commands written in higher level programming languages*". Così J. Krysa e G. SEDEK, *Source Code*, in M. FULLER (a cura di), *Software studies\ a lexicon*, MIT Press, Cambridge (MA), 2008, 237. Cfr. S. COUTURE, *The Ambiguous Boundaries of Computer Source Code and Some of Its Political Consequences*, in J. VERTESI, D. RIBES (a cura di), *digitalSTS: A Field Guide for Science & Technology Studies*, Princeton University Press, Princeton, 138.

[494] G. D'IPPOLITO, Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. Il caso dell'uso secondario di *Big Data*, 6, *Il diritto dell'informazione e dell'informatica*, 2018, 943, 954 il quale richiama le analoghe posizioni di M. BERTANI, *Diritti d'autore e connessi*, in L.C. UBERTAZZI (a cura di), *La proprietà intellettuale*, Giappichelli, Torino, 2011, 274 ss; M. BORGHI, *Owning Form, Sharing Content: Natural-Right Copyright in the Digital Environment*, in F. MACMILLAN (a cura di), *New Directions in Copyright Law*, Vol. 5, Cheltenham-Northampton, Edward Elgar, 2007, 197; G. CAVANI, *Oggetto della tutela*, in L.C. UBERTAZZI, *La legge sul software. Commentario sistematico*, Quaderni di Aida n.1, Milano, Giuffrè, 1994, 19ss.

[495] G. D'IPPOLITO, Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. Il caso dell'uso secondario di *Big Data*, 6, *Il diritto dell'informazione e dell'informatica*, 2018, 943, 956. Cfr. A.M. GAMBINO, R. PETTI, *Privacy e Proprietà Intellettuale*, in E. TOSI (a cura di), *Privacy*

Esclusa così la accessibilità del codice sorgente e del codice oggetto, si deve ricostruire in cosa altro possano concretamente consistere le idee alla base della logica seguita dal sistema di IA, non coperte dalla direttiva e il cui accesso è richiesto *ex* artt. 15 e 22 GDPR.

Come più volte ribadito, nel caso di ML non supervisionato le idee alla base del sistema non sono in grado di soddisfare la soglia minima di significatività richiesta dal GDPR, neppure per la fase pre-reclamo, poiché le categorie di variabili e il peso ad esse attribuito è generalmente stabilito dalla macchina nel corso del processo decisionale in modo autonomo, non prevedibile e non motivabile dal programmatore[496].

Sappiamo anche, però, che sebbene il diritto dell'interessato di conoscere la "logica cui risponde qualsiasi trattamento automatizzato […] non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software […], tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato *tutte* le informazioni"[497].

Quest'ottica di bilanciamento porta quindi a chiedersi se tale *empasse* sia superabile riconoscendo l'accesso all'algoritmo, quale espressione matematica della funzione poi svolta attraverso l'elaborazione del codice sorgente e oggetto, ovvero ammettendo la divulgazione dei profili stessi, intesi come risultato del processo decisionale automatizzato non coperto dal diritto d'autore.

Quanto al primo interrogativo, si può preliminarmente osservare che, non proibendo attività di *reverse engineering* se non nella forma della decompilazione

digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, Giuffré, 2019; A.M. GAMBINO, *Cloud, diritto d'autore e nuovi modelli di circolazione giuridica*, in AA.VV., *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza*, Milano, Giuffrè, 2019, 347SS; O. POLLICINO, M. BELLEZZA, *Tutela della privacy e protezione dei diritti di proprietà intellettuale in rete*, in O. POLLICINO, A.M. MAZZARO (a cura di), *Tutela del copyright e della privacy sul web: quid iuris?*, Roma, Aracne, 2012, 13 ss; A.M. GAMBINO, C. BOMPREZZI, Blockchain e protezione dei dati personali, in *Diritto dell'informazione e dell'Informatica*, 2019, 619 ss.

[496] "Si tratta di costrutti in italiano (o in inglese) studiati per assomigliare alle istruzioni di un linguaggio di programmazione, ma che in realtà non si eseguono su un computer. Lo pseudocodice rappresenta un compromesso tra i due estremi del linguaggio naturale di quello formale; è semplice, altamente leggibile e praticamente privo di regole grammaticali (n effetti, lo pseudocodice viene talvolta chiamato "linguaggio di programmazione senza dettagli")". Così, G.M. SCHNEIDER, J.L. GERSTING, *Informatica*, RN, Maggioli Editore, 2013, 37 ss.

[497] GDPR, considerando 63. Corsivo aggiunto.

(consistente nel risalire dal codice oggetto al codice sorgente)[498], la direttiva dir. 2009/24/CE sembrerebbe consentire lo sviluppo della funzione espressa dal medesimo algoritmo in un codice sorgente diverso ma strumentale all'esecuzione dello stesso compito. In questo senso, l'algoritmo in sé[499], dovrebbe ritenersi estraneo a qualsiasi forma di tutela autorale e liberamente appropriabile[500].

Non manca, tuttavia, chi ritiene l'algoritmo suscettibile di tutela ai sensi della dir. 2016/943/UE sulla protezione dei segreti commerciali[501]. Secondo quanto chiarito dal considerando 14 della dir. 2016/943/UE, infatti, tale nozione ricomprende non soltanto il *know-how*, ma anche le informazioni commerciali e tecnologiche[502] ove non

[498] Sull'ammissibilità di tecniche di "*black box analysis*" che non vadano oltre l'osservazione esterna del funzionamento del programma si veda G. GUGLIELMETTI, *Analisi e decompilazione dei programmi*, in L.C. UBERTAZZI, *La legge sul software. Commentario sistematico*, Quaderni di Aida n.1, Milano, Giuffrè, 1994, 159-160. Per una definizione si vedano le parole di Fumagalli "[…] [L]a decompilazione è il processo per cui, partendo dal codice in formato oggetto, si cerca di ricostruire il codice in formato sorgente, attraverso specifici *tools* informatici. La pratica del "*reverse engineering*", oltre alla decompilazione, prevede lo studio del software e la sua ricostruzione nelle parti più innovative, durante la sua esecuzione, attraverso l'uso di emulatori hardware, simulatori software di piattaforma, *debuggers*, etc." G. FUMAGALLI, *La tutela del software nell'Unione Europea. Brevetto e diritto d'autore*, Milano, Nyberg Edizioni, 2005, 57. Cfr. N. LUCCHI, *I Contenuti Digitali: Tecnologie, Diritti e Libertà*, Springer, 2010, 104 ss; E. BERLINGIERI, *Legge 2.0: il web tra legislazione e giurisprudenza*, Milano, Apogeo, 2008, 32 ss; M. FARINA, *I contratti informatici*, Milano, Editore Key, 2018, 32 ss.

[499] Nel contesto *Big Data* l'algoritmo è stato efficacemente definito come il costrutto matematico che descrive "*how* […] *orders and commands are practically implemented and combined into a particular program, software, or information system, with the ultimate goal of inferring from data the answers to be given to a specific set of questions*." M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018, 202, la quale richiama l'analoga formulazione utilizzata da R. HILL, What an algorithm is, 29, *Philosophy & Technology*, 1, 2015, 35, 37. Cfr. B.D. MITTELSTADT, P. ALLO, M. TADDEO, S. WACHTER, L. FLORIDI, *The ethics of algorithms: Mapping the debate*, *Big Data & Society*, 2, 2016, 1-21.

[500] Cfr. G. D'IPPOLITO, Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. Il caso dell'uso secondario di *Big Data*, 6, *Il diritto dell'informazione e dell'informatica*, 2018, 943, spec. nt 79 che richiama sul punto la tesi formulata da Pelino con riferimento alla posizione assunta da Trib. Bari Sez. IV, 14 marzo 2007, con nota di E. PELINO, Lecito commercializzare programmi simili, se si variano le procedure di sviluppo V, *Dir. internet*, 2007, 447.

[501] In questo senso si è chiaramente espressa al Commissione giuridica del Parlamento europeo nella persona del Rapporteur F. ZAMMIT DIMECH. ID., *Parere della commissione giuridica destinato alla commissione per il mercato interno e la protezione dei consumatori sulla proposta di regolamento del Parlamento europeo e del Consiglio che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online* (Parlamento europeo, 26 novembre 2018) - COM(2018)0238, 3. Cfr. G. MALGIERI e G. COMANDÈ, Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017, 243 ss.

[502] Come efficacemente osservato "con il know-how si hanno le conoscenze per fare qualcosa (creare un bene ovvero offrire un servizio)"; "con il segreto commerciale si hanno conoscenze esclusive nella fase di realizzazione industriale o della fornitura di un servizio"; "con le informazioni commerciali si hanno nozioni utili per la commercializzazione di un bene o di un servizio (ma non essenziali sul profilo industriale)". D. MASTRELIA, La tutela del know-how, delle informazioni e dei segreti commerciali fra novità normative, teoria e prassi, 5, *Diritto industriale*, 2019, 513, 514. Cfr. G. CRESPI, commento *sub* artt. 98-99 c.p.i, in A. VANZETTI (a cura di), Codice proprietà industriale, Milano, Giuffrè, 2013, 1101 ss; S. MAGELLI, Il know-how nell'esperienza giurisprudenziale italiana tra esclusiva e concorrenza sleale, 2, *Diritto Industriale*, 2016, 189 ss; V.M. DE SANCTIS, *I soggetti del diritto d'autore*, II ed., Milano, Giuffrè, 2005, 167ss.

generalmente note o facilmente accessibili, dotate di valore commerciale in quanto segrete e, per tal motivo, sottoposte a misure ragionevoli per tenerle tali[503].

Per quanto sia discusso in che misura gli algoritmi possano distinguersi dalle idee non monopolizzabili ai sensi della disciplina del diritto d'autore[504], ovvero in che misura siano sufficientemente inaccessibili da esperti, anche attraverso tecniche di *reverse engineering*, ai sensi della normativa sul *Trade Secret*[505], ai fini dell'analisi qui condotta, è sufficiente notare come l'algoritmo integri una forma di conoscenza difficilmente compatibile con lo standard di significatività come ricostruito nel precedente paragrafo, non soltanto perché non intellegibile per l'interessato medio, ma soprattutto perché estremamente generico ed astratto[506].

Esclusa così anche l'utilità, prima ancora che l'accessibilità, dell'algoritmo, si può concludere che, rispetto alla fase pre-reclamo, i doveri informativi di cui all'articolo 15 GDPR rispetto ai processi decisionali automatizzati potrebbero essere adeguatamente rispettati offrendo una descrizione ragionata, personalizzata e intelligibile dello pseudocodice. Quest'ultimo è inteso come quella forma di linguaggio naturale che i

[503] Articolo 2 pararagrafo 1 dir. 2016/943/UE, recepito nel nostro ordinamento dall'articolo 98 del codice della proprietà industriale, come novellato dal d.lgs. 63/2018.

[504] G.N. LA DIEGA, Le idee e il muro del suono. I programmi per elaboratore nella più recente giurisprudenza europea, 2, *Europa e dir. Priv*, 2013, 543, 552. Cfr. G. CICCONE e F. GHINI, La tutela giudiziale civile dei segreti commerciali anche dopo l'introduzione del d.lgs. n. 63/2018, 5, *Diritto industriale*, 2019, 529; F. BANTERLE, M. BLEI, Alcune novità introdotte dalla direttiva Trade Secrets, 4, *Diritto industriale*, 2017, 202ss.

[505] M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018, 207, la quale osserva come gli algoritmi volti ad implementare processi decisionali automatizzati debbano necessariamente prendere la forma di programmi per elaboratori, e quindi debbano essere formulati in codice sorgente, poi a sua volta tradotto in codice oggetto leggibile dall'elaboratore. Ai fini della normativa europea sul *Trade Secret*, tuttavia, la diversa forma assunta dall'algoritmo è irrilevante nella misura in cui tale informazione rimane segreta, ha un valore commerciale e vengono adottate misure adeguate a mantenere tale segretezza. I *raw data* hanno scarso valore nel contesto *Big Data* poiché il vantaggio competitivo è dato dall'abilità di inferire conoscenze con l'algoritmo. Per questo motivo Maggiolino sostiene che l'algoritmo rientra nell'ambito di applicazione dell'articolo 2 dir. 2016/943/UE.

[506] Per un'applicazione giurisprudenziale del difetto di motivazione legato all'oscurità dell'algoritmo, si veda *ex multis* Consiglio di Stato sez. VI, 02 luglio 2019, n. 4522; Consiglio di Stato sez. VI, 29 aprile 2019, n. 2764; Consiglio di Stato sez. VI, 19 marzo 2018, n. 1710; Consiglio di Stato sez. VI, 23 gennaio 2018, n. 447; Consiglio di Stato sez. VI, sent. 02 ottobre 2017, n. 4561. Per ulteriori riflessioni circa le posizioni assunte dal Consiglio di Stato, sez. VI, Sent. n.2270 dell'8 aprile 2019 e dalla sez. III-*bis* TAR Lazio con la sentenza n. 3769/2017 si veda quanto osservato *supra*, spec. nt. 203. Cfr. C. TABARRINI, Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019, 555 ss; L. VIOLA, L'Intelligenza Artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte, 2, *Foro Amministrativo*, 9, 2018, 1598.

programmatori utilizzano per sviluppare la bozza degli algoritmi da tradurre in codice sorgente, e che si colloca quindi a metà strada fra i due[507].

Spostando l'attenzione sulle esigenze di contestualizzazione poste dalla fase del reclamo, invece, e assunta l'impossibilità di risalire allo specifico peso relativo esercitato dalle varie informazioni effettivamente prese in considerazione dal sistema di ML non supervisionato per addivenire alla decisione (o per creare il gruppo), è necessario chiedersi se tale vuoto di tutela creato dalla insostenibilità tecnologica della normativa possa essere parzialmente colmato con l'accesso ai profili. Questi ultimi, come detto, pur non esprimendo l'intera logica algoritmica, sono comunque idonei a mettere l'interessato nella condizione di poter contestare la pertinenza degli assunti di base da cui ha preso le mosse il processo decisionale automatizzato[508].

Premettendo che ciò è possibile soltanto nella misura in cui il profilo sia il prodotto ultimo di un precedente trattamento automatizzato e non il prodotto intermedio di un unico processo decisionale automatizzato, ci si deve chiedere se i profili stessi possano essere qualificati come segreto commerciale ai sensi dell'articolo 2 dir. 2016/943/UE.

Come puntualizzato dal considerando 2 della direttiva, infatti, la protezione ivi disciplinata riguarda non soltanto il *know-how*, ma anche "un'ampia gamma di informazioni, che si estendono dalle conoscenze tecnologiche ai dati commerciali quali ad esempio le informazioni sui clienti e i fornitori, i piani aziendali e le ricerche e le strategie di mercato". Ciò in quanto, nell'"economia della conoscenza" le imprese investono nella produzione e sfruttamento di tali informazioni quali "moneta di scambio" e fonte di "vantaggio competitivo"[509].

---

[507] Come efficacemente descritto "[l]o pseudocodice è un linguaggio artificiale e informare che i programmatori adottano per mettere su carta gli algoritmi che hanno in mente, senza doversi preoccupare dei dettagli della sintassi di un linguaggio come il C++ [i.e. un linguaggio di programmazione]. […] I programmi scritti in pseudocodice, infatti, non sono destinati ai computer, ma agli uomini, e sono uno strumento valido per mettere nero su bianco le idee fondamentali di un algoritmo, prima di codificarlo con un linguaggio come il C++." H. M. DEITEL, P.J. DEITEL, *C++. Fondamenti di programmazione*, Maggioli Editore, 2014, 116.

[508] Cfr. GRUPPO DI LAVORO ARTICOLO 29, *Opinion 03/2013 on purpose limitation*, adottata il 2 aprile 2013 (00569/13/EN), 47.

[509] Dir. 2016/943/UE, considerando 1. Cfr. G. D'IPPOLITO, Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. Il caso dell'uso secondario di *Big Data*, 6, *Il diritto dell'informazione e dell'informatica*, 2018, 943. L'Autore sottolinea come il recente sviluppo economico, dominato sempre più dal ruolo delle piattaforme digitali quali nuovi modelli di "*two-sided market*", vede nella raccolta massiva e successiva rielaborazione di dati uno dei suoi elementi più vitali tanto da poter parlare ormai di "economia dei dati" e di "*knowledge-based economy*". Ciò è tanto più vero con riferimento

In quest'ottica, se "il semplice elenco dei nominativi di clienti ed i relativi indirizzi fisici e virtuali, che sia privo di ulteriori informazioni qualificanti del singolo cliente, non costituisce segreto aziendale *ex* artt. 98-99 c.p.i. stante la mancanza di uno specifico valore economico nell'esercizio dell'attività imprenditoriale dei dati in questione"[510], *a contrario*, i profili inerenti preferenze e altri tratti della personalità di gruppi di clienti o potenziali clienti, in quanto prodotto di consistenti investimenti e fonte di valore economico (ove non generalmente accessibili), possono ben qualificarsi come segreto commerciale[511].

Ne consegue che, se la definizione di segreto commerciale non dovrebbe "imporre restrizioni sull'oggetto da proteggere", e nella misura in cui quest'ultimo può essere rappresentato da qualsiasi risorsa suscettibile di tradursi in un vantaggio competitivo se mantenuta segreta[512], i profili non possono che godere della protezione accordata dalla direttiva 2016/943/UE.

Sebbene la direttiva sulla protezione dei segreti commerciali non crei "alcun diritto esclusivo sul *know-how* o sulle informazioni che godono di protezione in quanto segreti commerciali" e ammetta "la scoperta indipendente dello stesso *know-how* o delle

ai cc.dd. soggetti "*Over the top*" per i quali informazioni e dati (personali e non) diventano asset importanti nei rispettivi *business model*.

[510] D. MASTRELIA, La tutela del know-how, delle informazioni e dei segreti commerciali fra novità normative, teoria e prassi, 5, *Diritto industriale*, 2019, 513, 521. Cfr. V. FALCE, Dati e segreti. Dalle incertezze del Regolamento Trade secret ai chiarimenti delle Linee Guida della Commissione UE, 2, *Diritto industriale*, 2018, 155 ss; A. FRIGNANI, Segreti d'impresa (voce), *Digesto*, IV, Disc. Priv. Sez. Comm., vol. XIII, 1997, 334 – 354. Si veda anche Tribunale Bologna Sez. spec. in materia di imprese, 4 luglio 2017, con nota di A. ANDOLINA, Tutela delle liste clienti tra concorrenza sleale, segreto industriale e banche dati, 5, *Giur. It.*, 2018, 1145 ss.

[511] Confermato da considerando 14 Dir. 2016/943/UE per cui "la definizione di segreto commerciale esclude le informazioni trascurabili, l'esperienza e le competenze acquisite dai dipendenti nel normale svolgimento del loro lavoro, ed esclude altresì le informazioni che sono generalmente note o facilmente accessibili alle persone all'interno delle cerchie che normalmente si occupano del tipo di informazioni in questione".

[512] A riprova dell'ampiezza del raggio di tutela offerto dalla normativa sul segreto commerciale viene richiama la giurisprudenza italiana che aveva ricompreso nella nozione di informazioni commerciali segrete le tecniche di *marketing* e di profilazione della clientela (Trib. Torino 6 luglio 2012, in *Giur. ann. dir. ind., 2013*, 591), nonché l'*Impact Assessment* della Commissione europea ove vengono individuate quattro categorie di informazioni proteggibili come *trade secrets*: "(i) segreti relativi a prodotti altamente specializzati (in questo caso il segreto coincide con il prodotto stesso); (ii) segreti tecnologici; (iii) informazioni commerciali strategiche; e (iv) raccolte di dati pubblicamente disponibili ma riarrangiati in maniera originale". M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018, 206; *Commission staff working document Impact Assessment accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets)* (Bruxelles, 28 novembre 2013) SWD(2013) 471 fin., 109 ss.

stesse informazioni"[513], l'impossibilità tecnologica di effettuare un *reverse engineering* della gran parte dei processi decisionali automatizzati rende questo varco normativo impercorribile ai fini informativi di cui all'articolo 22 GDPR.

Ciononostante, pur riconoscendo la pervasività della protezione accordata ai sistemi di IA dai vari livelli di proprietà intellettuale, rimane inalterata l'esigenza di trovare una opzione di *disclosure* tecnologicamente fattibile e giuridicamente in grado di bilanciare il rispetto degli interessi economici dei detentori di diritti di proprietà intellettuale sui software di AI utilizzati per implementare il processo decisionale automatizzato, con il diritto degli interessati a veder osservate le tutele garantire dal GDPR[514].

Come più volte ribadito[515], infatti, l'esigenza di bilanciare i diritti di privativa industriale del titolare del trattamento con il diritto di accesso alla logica algoritmica non viene meno per effetto del processo di clusterizzazione dei dati. La natura fiduciaria del ruolo che il titolare viene a rivestire nei confronti dell'interessato rispetto al trattamento dei suoi dati non cessa quando questi assumono una dimensione di gruppo, con la conseguenza che i doveri di cura che il GDPR fissa in relazione al singolo dato personale non possono che dover essere estesi al profilo, in quanto proiezione del singolo frammento informativo nella sua dimensione collettiva. Ne consegue che la mera natura artificiale e sovraindividuale delle informazioni confluite nel profilo non può di per sé giustificare un diniego di accesso al profilo in quanto segreto industriale esorbitante dall'ambito di applicazione del GDPR.

In ottica di tale bilanciamento, quindi, una prima soluzione, sicuramente audace e forse troppo drastica, potrebbe essere quella di sfruttare le caratteristiche tecnologiche dei processi decisionali alimentati da ML, per rendere inapplicabile la disciplina sulla proprietà intellettuale. Ad esempio, parte della dottrina ha acutamente osservato come il vaglio di sussistenza del requisito della segretezza del segreto commerciale imponga la

[513] Considerado 15 Dir. 2016/943/UE. Nello stesso senso si esprime M. Maggiolino, secondo la quale "*the holder of a trade secret cannot prevent others from reaching out the same knowledge and information by way of "independent discovery or creation*" M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018, 210.

[514] In questo senso si esprimono il considerando 34 dir. 2016/943/UE, in virtù del quale "La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta, nella fattispecie il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali."

[515] V. *supra sub* §1.6.

possibilità di verificare in concreto se tali conoscenze siano effettivamente "non generalmente note" o "non facilmente accessibili". In quest'ottica, non si può che condividere la posizione di chi ha escluso "la tutela dei sistemi di intelligenza artificiale opachi (c.d. *black box*) ove i modelli di regole, in cui si articola il processo decisionale del sistema, possono rimanere inconoscibili allo stesso titolare, impossibilitato talvolta a effettuare perfino un *self-reverse engineering*" [516].

Un altro percorso esegetico potrebbe essere quello di ammettere la tutela del codice sorgente e del codice oggetto del sistema di ML, ma negare protezione a tutti i prodotti del processo decisionale automatizzato, inclusi i profili, in quanto risultato del solo ingegno della macchina, in alcun modo imputabile al programmatore. In altri termini, se si muove dal presupposto per cui il segreto commerciale ha "lo stesso valore dei brevetti e di altre forme di diritto di proprietà intellettuale"[517], la sua tutela non può che essere limitata alle fattispecie in cui sia individuabile un autore umano. Nonostante la diversa posizione assunta da alcune legislazioni nazionali, infatti, la normativa europea, così come la dottrina maggioritaria, ritengono giuridicamente impossibile riconoscere diritti di proprietà intellettuale su opere o invenzioni cc.dd. "*computer-generated*". Ciò in quanto, ove anche fosse possibile riconoscere ai sistemi di ML la capacità di produrre *output* originali, la mancanza di soggettività giuridica in capo ai sistemi di Intelligenza Artificiale, anche se in versione *deep learning* e non supervisionata, rende legislativamente impossibile individuare un autore dotato della capacità giuridica necessaria ad essere titolare dei diritti che da tale protezione discenderebbero[518].

[516] L'Autore prosegue poi notando come l'opzione interpretativa riportata nel testo, "volta al contenimento delle possibili tendenze indebitamente espansive del segreto sulla base di una lettura teleologica dei requisiti, non pare invece potersi spingere al punto di escludere la tutela del diritto per il solo fatto che la conoscenza considerata attenga a fenomeni della realtà singolarmente accessibili da terzi." A. OTTOLIA, Il D.Lgs. N. 63/18 di attuazione della Dir. 2016/943/Ue sulla protezione dei segreti commerciali fra tutela e bilanciamenti, 5, *Nuove leggi civili commentate*, 2019, 1091, 1102.

[517] Così si esprime il considerando 2 della dir. 2016/943/UE. Cfr. M.A. LEMLEY, The Surprising Virtues of Treating Trade Secrets as IP Rights, 61, *Stanford Law Review*, 2, 2008, 311, 314. In senso analogo Ottolia, per il quale "[d]a strumento di tutela di un valore intrinsecamente, e staticamente, connesso all'azienda e alla sua dialettica competitiva, il segreto è divenuto un altro mezzo per "appropriarsi dei risultati delle attività innovative" al pari di altri diritti di proprietà intellettuale ed è stato pertanto più compiutamente riconosciuto nella sua prospettiva dinamica, che afferisce al valore di una conoscenza (segreta ma) suscettibile di circolare nel mercato secondo una logica che pare non più compatibile con la delimitazione imprenditoriale dei soggetti tutelati". A. OTTOLIA, Il D.Lgs. N. 63/18 di attuazione della Dir. 2016/943/Ue sulla protezione dei segreti commerciali fra tutela e bilanciamenti, 5, *Nuove leggi civili commentate*, 2019, 1091,1096.

[518] Sul tema della personalità giuridica dei sistemi di Intelligenza Artificiale si vedano, fra tutti, C.E.A. KARNOW, The Encrypted Self: Fleshing Out the Rights of Electronic Personalities, 13, *Journal of Computer & Information Law*, 1994, 1; L.B. SOLUM, Legal Personhood for Artificial Intelligences, 70, *N.C.*

Ne consegue che, *de iure condito*, i profili inferiti da sistemi di ML non supervisionato, pur se astrattamente suscettibili di essere qualificati come informazioni commerciali ai sensi della direttiva 2016/943/UE, non possono godere della tutela ivi accordatagli nella misura in cui risultino il prodotto di scelte non predeterminate né prevedibili dal programmatore, e quindi sostanzialmente libere, creative ed esclusivamente imputabili alla macchina.

Infine, ove anche tale tentativo ermeneutico dovesse essere considerato fallimentare, la possibilità per l'interessato di avere accesso al profilo in fase di reclamo potrebbe riconoscersi interpretando estensivamente le cautele introdotte dal legislatore nell'ambito di procedimenti giurisdizionali aventi ad oggetto segreti commerciali, proprio in ottica di contemperamento di interessi[519].

Il considerando 24 dir. 2016/943/UE, infatti, sottolinea la necessità di stabilire "opportune misure di salvaguardia intese a garantire il diritto a una tutela effettiva e a un processo equo, prescrizioni specifiche volte a tutelare la riservatezza del segreto commerciale oggetto di contenzioso nel corso dei procedimenti giudiziari avviati per la sua difesa". A tal fine, l'articolo 9 paragrafo 1 consente all'autorità giudiziaria, su richiesta motivata della parte interessata, di porre un vincolo di riservatezza sulla documentazione processuale, conseguentemente vietandone l'utilizzo e la divulgazione da parte tutti i soggetti che ne hanno avuto accesso nel corso del procedimento, anche dopo la conclusione dello stesso. Lo strumentario del giudice è poi ulteriormente arricchito dal nuovo articolo 121 *ter* c.p.i. che, in attuazione della direttiva, attribuisce al giudice anche la possibilità di adottare misure volte a restringere l'accesso fisico alle

L. Rev., 1992, 1231, e C.D. STONE, *Should Trees Have Standing? Law, Morality, and the Environment*, III ed., Oxford University Press, Oxford, 2010, 8ss; G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Edizioni Scientifiche Italiane, Napoli, 2019, 36ss; W. BARFIELD, Towards a Law of Artificial Intelligence, in W. BARFIELD e U. PAGALLO (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Northampton, 2018, 36 ss.

[519] La posizione è condivisa anche da Maggiolino, la quale nota come seppure sia assente una norma che imponga un generalizzato dovere di *disclosure* in capo ai detentori di un segreto commerciale, si deve ammettere che ove un soggetto ritenga un algoritmo segreto responsabile di illecito, potrà avviare una procedimento giurisdizionale nell'ambito del quale le autorità competenti devono avere la possibilità di scrutinare il funzionamento dell'algoritmo stesso (come avvenuto nel caso Google Shopping ad opera della Commissione europea). M. MAGGIOLINO, *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018, 211. Cfr. *Microsoft Corp. v Commission of the European Communities*, Case T-201/04, ECLI:EU:T:2007:289.

udienze, come agli atti e documenti del fascicolo d'ufficio, nonché a oscurare i contenuti sensibili inclusi nei provvedimenti emessi[520].

In conclusione, interpretando l'obbligo del titolare di "fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati" alla luce di tale quadro normativo e della più volte ricordata natura fiduciaria del rapporto titolare-interessato, si sostiene che, il diritto di quest'ultimo a contestare la decisione unicamente automatizzata *ex* art. 22 GDPR possa essere rispettato riconoscendogli l'accesso ai profili, in quanto unica fonte di conoscenza tecnologicamente sostenibile e giuridicamente "significativa". Allo scopo, e nella misura in cui il dovere di trasparenza disciplinato dall'articolo 22 GDPR prescinde dall'esercizio di un'azione giurisdizionale[521], il titolare sarà tenuto ad implementare procedure interne di reclamo che, al pari di quanto previsto dalla direttiva Omnibus,[522] e seppure con le cautele di cui alla direttiva 2016/943/UE, consentano all'interessato di avere accesso a tutte le informazioni tecnologicamente recuperabili e necessarie consentigli di chiarire e contestare i fatti e le circostanze specifiche alla base della decisione automatizzata.

[520] Cfr. G. CICCONE e F. GHINI, La tutela giudiziale civile dei segreti commerciali anche dopo l'introduzione del d.lgs. n. 63/2018, 5, *Diritto industriale*, 2019, 531, i quali notano come in tale ottica si inquadrino anche le cc.dd. *cleaning rooms*, ovvero procedure di scrematura documentale condotte alla sola presenza dei legali e dei consulenti di parte e d'ufficio al fine di minimizzare il rischio di divulgazione involontaria di informazioni riservate, senza compromettere l'efficacia del vaglio del giudice e delle esigenze di difesa delle parti. Cfr. F. BANTERLE, M. BLEI, Alcune novità introdotte dalla direttiva Trade Secrets, 4, *Diritto industriale*, 2017, 202ss.

[521] Sull'obbligo di adottare misure tecniche e organizzative interne di minimizzazione di eventuali errori ed effetti discriminatori si veda quanto stabilito dal considerando 71 GDPR.

[522] In questo senso si ricorda quanto sancito dal Regolamento (UE) 2019/1150 del Parlamento Europeo e del Consiglio del 20 giugno 2019 che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online, G.U. L 186/57, Considerando 22.

CAPITOLO TERZO

LA DISCIPLINA DEI PROCESSI DECISIONALI AUTOMATIZZATI NEL CONTESTO DELLA *DATA PRIVACY* STATUNITENSE

SOMMARIO: 3.1. Il Privacy Shield *e l'astensione dalla valutazione di adeguatezza della disciplina dei processi decisionali automatizzati negli Stati Uniti - 3.2. La matrice dominicale della* proprietary privacy *- 3.3. Il* Katz test*: per una privacy delle persone e non dei luoghi - 3.4. La (non) ragionevolezza dell'aspettativa di privacy nella rete - 3.4.1. La* plain-sight doctrine *come limite alla riservatezza di informazioni archiviate sul proprio* personal computer *- 3.4.2. La* Third-Party Doctrine *come limite alla riservatezza delle informazioni gestite da* Internet Service Providers *- 3.5.* Electronic Communication Privacy Act*: un divieto di intercettazioni unicamente automatizzate? - 3.6. La "spiegazione" delle decisioni prese nel contesto della* Credit Reporting Industry *- 3.6.1. La* consumer disclosure *del* Financial Credit Reporting Act *- 3.6.2. I doveri di* adverse action notice *dell'*Equal Credit Opportunity Act *- 3.7. Il* due process *come limite alla legittimità di processi decisionali automatizzati "opachi" - 3.8. Il ruolo della* Federal Trade Commission *in ambito di* data privacy *- 3.8.1. La potestà legislativa della FTC: il futuro della data privacy statunitense? - 3.9. Verso la trans-settoriale della data privacy: il California* Consumer Privacy Protection Act *e gli* ALI Data Privacy Principles.

3.1. Il Privacy Shield e l'astensione dalla valutazione di adeguatezza della disciplina dei processi decisionali automatizzati negli Stati Uniti

Il crescente flusso transfrontaliero di dati personali, principalmente riconducibile all'oligopolistico mercato digitale controllato dai GAFAA, rende imprescindibile l'assunzione di una prospettiva comparatistica nell'analisi giuridica del fenomeno. Ciò non tanto all'ancora utopico fine di individuare un regime normativo uniforme di tutela dei dati, quanto al più modesto scopo di meglio comprendere le dinamiche internazionali innescate dall'intensificarsi dei traffici transfrontalieri dei dati.

Se le vicende Snowden e Schrems hanno insegnato qualcosa è proprio come l'instaurazione di un contesto di mutuo intendimento tra Stati sia presupposto imprescindibile per l'effettiva implementazione di un regime internazionale di protezione dei dati provenienti dall'Unione europea. In quest'ottica, la concentrazione in suolo nordamericano di grandissima parte dei *Bigtechs* protagonisti della c.d. quarta rivoluzione

industriale e membri fondatori dell'economia dei dati, rende scontata, quanto obbligata, la scelta dell'ordinamento statunitense quale oggetto di analisi e raffronto.

A tal fine, muovendo da una fondamentale premessa terminologica, si mette fin d'ora in evidenza come negli Stati Uniti la nozione eurounitaria di protezione dei dati personali sia generalmente tradotta col concetto di *informational privacy* (sottocategoria della *proprietary privacy*), più comunemente nota anche come *data privacy*[523].

Dal punto di vista sostanziale e metodologico, invece, è necessario premettere alcune principali differenze tra il quadro normativo eurounitario e quello statunitense, la prima delle quali è rinvenibile nella circostanza per cui mentre il primo si configura come prevalentemente legislativo e tecnologicamente neutrale ("*technology-independent*"), l'approccio nordamericano è tradizionalmente giurisprudenziale, casistico e, per tal motivo, anche inevitabilmente "*technology-dependent*"[524].

Come correttamente osservato, inoltre, altra importante differenza è rinvenibile nella marcata diffidenza che gli europei manifestano verso lo sfruttamento commerciale dei dati personali da parte di soggetti privati, quasi assente nella cultura nordamericana, molto più attenta, invece, alla salvaguardia della propria privacy rispetto a interferenze abusive da parte del governo (federale e statale)[525].

Per questo motivo, a dispetto del ruolo centrale svolto dalla dottrina e dalla giurisprudenza statunitense nel percorso di affermazione dell'originaria nozione di privacy, e nonostante l'accresciuta influenza che l'evoluzione della disciplina eurounitaria in materia di protezione dei dati personali è venuta ad esercitare oltreoceano per effetto dell'intensificarsi del flusso transfrontaliero di dati, negli Stati Uniti continua

[523] P.P. SWIRE e K. AHMAD, *Foundations of Information Privacy And Data Protection*, International Association of Privacy Professionals, Portsmouth, 2012, 4; S. COBB, *Data privacy and data protection: US law and legislation*, ESET White Paper, 2016; S.M. BOYNE, *Data Protection in the United States: U.S. National Report*, in D. M. VICENTE e S. DE VASCONCELOS CASIMIRO (a cura di), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law, Vol. 38, Springer, Cham, 2020, 410 ss.

[524] D. KLITOU, *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014, 40 ss.

[525] S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299, 343 spec. nt. 317, dove viene richiamato il pensiero di B. SULLIVAN, *La difference Is Stark in **EU,** U.S. Privacy Laws* (NBC NEWS, 19 ottobre 2006), disponibile su www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws. Cfr. G. RESTA, La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE, in *Dir. Inf. e inform.*, 2015, 697ss.

a mancare una legislazione federale onnicomprensiva in materia di privacy e protezione dei dati personali[526]. Il complesso delle fonti in materia di trattamento dei dati personali (specialmente a fini commerciali), infatti, è altamente lacunoso e costituito da poche leggi federali settoriali[527], sporadici interventi dei legislatori statali e forme di autoregolamentazione rinforzate dalla vigilanza della *Federal Trade Commission* (FTC)[528].

A livello federale, manca la previsione di generali diritti di accesso o di cancellazione dei dati, così come di espressi doveri informativi (ad esempio di notifica di *data breach*) e di basi giuridiche per il trattamento, prima fra tutte quella del previo consenso informato dei soggetti interessati[529]. Le società di *Data Analytics* e agenzie di *Data Brokerage* operano quindi in un contesto prevalentemente privo di vincoli legislativi[530].

Tale vuoto normativo, tuttavia, non ha impedito a parte della dottrina di ritenere addirittura più garantista l'ordinamento statunitense, perlomeno in materia di perquisizioni, intercettazioni, utilizzo di prove illegalmente ottenute, nonché di accesso alle comunicazioni elettroniche [531]. Eppure, la forte attenzione storicamente prestata dal legislatore e dalle corti statunitensi ai limiti delle ingerenze pubbliche nella sfera di riservatezza dei cittadini non ha ostacolato l'affermarsi di pratiche di sorveglianza

[526] Per riflessioni sull'evoluzione del rapporto tra la disciplina vigente negli USA e nell'UE in materia di protezione dei dati personali si veda P.M. SCHWARTZ, The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures, 126, *Harv. L. Rev*., 2013, 1966ss.

[527] Sul carattere frammentato e settoriale della legislazione statunitense sulla protezione dei dati personali si veda, fra gli altri, I. Berle, Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal, Law, Governance and Technology Series, Springer, Cham, 2020, 93ss.

[528] Per un'analisi del contenuto tipico e dell'efficacia delle tradizionali formulazioni contenute nelle privacy policies di matrice statunitense si veda J. FERNBACK, Z. PAPACHARISSI, Online privacy as Legal Safeguard: The Relationship Among Consumer, Online Portal, and Privacy Policies, 9, *New Media & Society*, 5, 2007, 715ss. Cfr. C. BENNETT e D. MULLIGAN, *The Governance of Privacy Through Codes of Conduct: International Lessons for U.S. Privacy Policy*, 2012, disponibile su *dx.doi.org/10.2139/ssrn.2230369*; S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299; D. SOLOVE e P.M. SCHWARTZ, *Information Privacy Law*, VI ed., Aspen Casebook Series, Wolters Kluwer, New York, 2018, 36-39; P.M. SCHWARTZ, Global Data Privacy: The EU Way, 94, *N.Y.U. L. REV*., 2019, 771, 772-73.

[529] J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J*., 23, 2019, 23, 29.

[530] Cfr. A.C. RAUL, C.C. FRONZONE e S.S. TAPIA, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 400 ss.

[531] P. SWIRE e D. KENNEDY-MAYO, How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information, 55, *EMORY L.J*., 2017, 617, 642.

elettronica talmente invasive da provocare l'invalidazione del *Safe Harbor Agreement*[532] e, più recentemente, anche del c.d. "scudo UE-USA per la privacy" (d'ora in avanti *Privacy Shield*)[533].

Esula dallo scopo della presente analisi la puntuale rievocazione delle vicende di cronaca susseguitesi all'indomani dello scandalo "*Datagate*". Basti qui ricordare come a seguito delle rivelazioni dell'ex agente della NSA sul programma di sorveglianza di massa noto come PRISM, la Corte di Giustizia dell'Unione europea sfruttò l'occasione offerta dal rinvio pregiudiziale operato dall'Alta corte irlandese nel caso *Maximillian Schrems contro Data Protection Commissioner* per dichiarare l'inadeguatezza del livello di protezione dei dati personali assicurato negli Stati Uniti[534]. In particolare, chiarì la Corte, sebbene l'ordinamento di destinazione del trasferimento di dati provenienti dall'Unione europea non debba presentare una disciplina formalmente sovrapponibile a quella eurounitaria, deve comunque offrire un regime di tutela dei diritti fondamentali sostanzialmente equivalente a quello oggi garantito dal GDPR, letto alla luce della Carta dei diritti fondamentali[535].

---

[532] Decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (GU L 215 del 28.8.2000). Per riflessioni sulle difficoltà che il sistema di *check and balances* statunitense ha incontrato nel settore della sicurezza nazionale, specialmente nell'affrontare l'ascesa di *BigTechs* quali Facebook e Amazon, si veda A. DEEKS, Facebook Unbound?, 105, *Va. L. Rev. Online*, 2019, 3ss. Cfr. M.C. MENEGHETTI, *Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017, 423 ss. Più in generale, sul contenuto del previgente accordo si veda, fra gli altri, S. SICA, V. D'ANTONIO, I *Safe Harbour Privacy Principles*: Genesi, Contenuti, Criticità, *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, 801ss.

[533] Decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 a norma della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, G.U.U.E. L 207/1 [d'ora in avanti Scudo UE-USA per la privacy], §§ 7-12. Cfr. F. ROSSI DAL POZZO, La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal *Safe Harbour* al *Privacy Shield*), *Rivista di Diritto Internazionale*, 3, 2016, 690ss.

[534] CGUE, sent. del 6 ottobre 2015 *Maximillian Schrems c. Data Protection Commissioner* C-362/14, ECLI:EU:C:2015:650, § 39. Cfr. R. BIFULCO, La sentenza Schrems e la costruzione del diritto europeo della privacy, in *Giur. Cost*., 2016, 289 ss; G. FINOCCHIARO, La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems, in *Dir. Inf. E inform*., 2015, 779 ss; A. MANTELERO, L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU e USA. Quali scenari per cittadini ed imprese?, in *Contratto e impresa./Europa*, 2015, 719 ss; V. ZENO-ZENCOVICH, Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in *Dir. inf. E inform*., 2015, 683 ss.

[535] In particolare, nel definire il contenuto minimo dei principi sostanziali necessari a soddisfare il vaglio di adeguatezza della Commissione, il Gruppo di Lavoro ha attribuito fondamentale rilievo all'esistenza nell'ordinamento del Paese terzo di: (i) una serie di concetti e nozioni base quali quelle di "dati personali", "trattamento", "titolare del trattamento", *etc.*; (ii) una chiara indicazione delle basi giuridiche

Preso così atto della "necessità di rivedere e rafforzare il fondamento stesso del regime dell'approdo sicuro", il 12 luglio 2016 la Commissione europea adottò il nuovo P*rivacy Shield*. Tale decisione, recentemente affiancata dal problematico *Clarifying Lawful Overseas Use of Data Act* (meglio noto come *CLOUD Act*)[536], ebbe l'effetto di

idonee a rendere i trattamenti leciti; (iii) limiti alle finalità del trattamento; (iv) principi volti a garantire il rispetto di canoni di correttezza, aggiornamento e necessarietà del dati trattati; (v) principi volti a garantire il rispetto di un canone di minimizzazione dei dati; (vi) regole di condotta deputate ad assicurare la sicurezza dei dati e prevenire accessi non autorizzati agli stessi; (vii) diritti informativi idonei ad assicurare un certo grado di trasparenza del trattamento; (viii) diritti di accesso, rettifica, opposizione e cancellazione dei dati; (ix) limitazioni al trasferimento dei dati verso soggetti terzi; (x) specifiche salvaguardie a tutela di particolari categorie di dati (come quelli sensibili); (xi) diritti di opposizione a trattamenti finalizzati a marketing personalizzato; (xii) condizioni di liceità di processi decisionali unicamente automatizzati e relativi diritti di conoscenza della logica seguita, di rettifica di eventuali erroneità nei dati utilizzati e di contestare decisioni assunte sulla base di presupposti fattuali scorretti. Dal punto di vista procedurale, invece, nel definire le caratteristiche minime di effettività dell'infrastruttura di *enforcement*, il Gruppo di Lavoro ha ribadito la necessità di rinvenire nell'ordinamento del paese terzo: (i) una autorità indipendente e imparziale competente a monitorare e far rispettare la normativa in materia di protezione dei dati; (ii) adeguati strumenti di *compliance* e sensibilizzazione degli operatori del settore quali ispezioni e misure sanzionatorie; (iii) misure di responsabilizzazione degli operatori volte ad imporgli la conduzione di valutazioni d'impatto o altre procedure intere idonee a consentirgli l'assolvimento dell'onere probatorio a loro carico in punto di compliance; (iv) rimedi effettivi volti a sanzionare violazioni accertate e riconoscere agli interessati risarcimenti per i danni eventualmente subiti. GRUPPO DI LAVORO ARTICOLO 29, *Adequacy Referential*, adottato il 29 novembre 2017, aggiornato al 6 febbraio 2018, (WP 254 rev.01), 3-9 adottato in revisione del WP12, *Working Document: Transfers of personal data to third countries. Applying Articles 25 and 26 of the EU data protection directive*, adottato il 24 luglio 1998. CGUE, sent. 6 ottobre 2015, causa C-362/14, *Maximilian Schrems c. Data Protection Commissioner*, EU:C:2015:650, 73-74. Cfr. F. BORGIA, Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 965.

[536] Esulando dallo scopo della presente analisi una puntuale disamina delle complesse problematiche sollevate dalla recente adozione del CLOUD Act, è sufficiente, in questa sede, notare come tale intervento legislativo abbia sostanzialmente superato la disciplina del *Mutual Legal Assistance Treaty* (MLAT) ammettendo la possibilità che le Corti statunitensi possano autorizzare (*rectius* ordinare) *Internet Service Providers* a fornire accesso a informazioni da essi digitalmente archiviate, seppure in *servers* collocati al di fuori del territorio degli Stati Uniti (così si è espressa la Corte Suprema nel recente caso *United States v. Microsoft Corp*., 584 U.S. ___ (2018)) . Allo stesso tempo, tuttavia, è prevista anche la possibilità di riconoscere analoghi poteri di accesso in capo a Stati terzi attraverso la stipula di appositi accordi intergovernativi. In attesa di ulteriori sviluppi sulle concrete conseguenze operative di tale nuovo regime, la portata extraterritoriale della normativa ha già suscitato le forti perplessità dello *European Data Protection Board*, che, nella sua *Joint Response on the US Cloud Act*, pur riconoscendo la necessità di modernizzare la disciplina dell'accesso transfrontaliero a materiale probatorio elettronico nel contesto di indagini attualmente dettato dal MLAT, ha ritenuto sostanzialmente illegittima la soluzione unilaterale di un "*US CLOUD Act warrant*" in mancanza di accordo internazionale sul punto. *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence* (EUROPEAN DATA PROTECTION BOARD, Bruxelles, 10 luglio 2019). Interessante a tal proposito anche la recente pronuncia con cui la Cassazione penale italiana, disattendo la tesi difensiva, ha ribadito la possibilità di acquisire materiale probatorio costituito da messaggistica scambiata a mezzo BlackBerry senza rogatoria internazionale, poiché aventi ad oggetto comunicazioni avvenute da terminale collocato sul suolo nazionale e decriptate con la spontanea collaborazione del produttore del dispositivo, quest'ultimo sì, collocato all'estero. Da notare, tuttavia, che ove tale supporto fosse venuto a mancare, l'acquisizione dei dati telematici (pur prodotti sul territorio nazionale) non sarebbe potuta avvenire in mancanza di rogatoria. Così Cass. penale, sez. III, sentenza del 13 maggio 2020, n. 14725. Cfr. V.P. MUSKIN, The Right to Be Forgotten, 91, *Mar N.Y. St. B.J*., 2019, 36, 38; R.M. GERACI, La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento *E-Evidence*, 3, *Cassazione Penale*, 2019, 1340ss; J. DASKAL, Microsoft Ireland, the Cloud Act, and International Lawmaking 2.0, 71, *Stan. L. Rev. Online*, 9, 10ss.

(ri-)autorizzare il trasferimento di dati personali verso le organizzazioni che, stabilite negli USA, avessero autocertificato il proprio impegno al rispetto dei principi del regime del *privacy shield*[537]. Anche quest'ultimo, tuttavia, è stato recentemente invalidato dalla Corte di giustizia dell'Unione europea che, nel decidere il c.d. caso Schrems II[538], ha rilevato come la persistente mancanza di limiti all'autorizzazione di alcuni dei programmi di sorveglianza attivi negli Stati Uniti, così come la carenza di garanzie per gli stranieri potenzialmente interessati da siffatte attività di monitoraggio elettronico, ne consentano un'implementazione ben oltre quanto strettamente necessario e perciò incompatibile col principio europeo di proporzionalità[539]. Ne è conseguito che, fatta invece salva la decisione 2010/87, il trasferimento di dati personali dall'Unione europea verso gli Stati Uniti potrà proseguire sulla scorta di Clausole Contrattuali Standard o delle Norme Vincolanti d'Impresa soltanto ove l'esportatore e l'importatore dei dati abbiano predisposto delle misure supplementari idonee a garantire un livello di protezione equivalente a quello fissato nell'Unione e non neutralizzabili dalle leggi vigenti nell'ordinamento di destinazione[540].

Alla luce di quanto sin qui premesso, lo scopo del presente capitolo è quello di analizzare se, ed in che misura, l'ordinamento statunitense offra garanzie adeguate (*rectius* equivalenti) a quelle di cui all'articolo 22 GDPR. A tal riguardo si deve innanzitutto notare come la Commissione europea, muovendo dal presupposto dell'esistenza negli Stati Uniti di legislazioni che, seppure a livello squisitamente settoriale, prevedono tutele specifiche contro decisioni sfavorevoli astrattamente idonee

[537] Scudo UE-USA per la privacy, §§ 14-15; S. SALUZZO, Cross Border Data Flows and International Trade Law the Relationship Between EU Data Protection Law and the GATS, *Diritto del Commercio Internazionale*, 4, 2017, 807ss.

[538] Sentenza della Corte di Giustizia dell'Unione europea (Grande Sezione) del 16 luglio 2020, causa C-311/18 Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems (ECLI:EU:C:2020:559). Cfr. E. TEROLLI, Privacy e protezione dei dati personali IE vs USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II", *Diritto dell'informazione e dell'informatica*, 1, 2021, 49 ss.

[539] La Corte ha inoltre ritenuto che il meccanismo di mediazione previsto dalla decisione 2016/1250 non offrisse garanzie sufficienti ad assicurarne un adeguato grado di indipendenza del Mediatore e la sua capacità di vincolare i servizi di intelligence statunitensi con le sue decisioni. Al contrario, la natura contrattuale, e quindi non vincolante per le Autorità del Paese terzo destinatario del trasferimento dei dati, non è stata considerata dalla Corte di per sé idonea ad invalidare la decisione 2010/87 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi.

[540] Quali siano, in concreto, esempi di misure normative, tecnologiche o organizzative supplementari allo scopo implementabili è una questione attualmente al vaglio dello *European Data Protection Board* (EDPB). Questo è, perlomeno, quanto chiarito nelle *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* adottate il 23 luglio 2020.

a tutelare gli interessati avverso decisioni unicamente automatizzate prese nei loro confronti da organizzazioni private, non aveva riprodotto il regime di cui all'articolo 22 GDPR in alcun principio del *Privacy Shield*. Analoga lacuna, peraltro, è rinvenibile nell'ordinamento statunitense nel quale non vige alcun divieto generale di adozione di decisioni unicamente automatizzate[541]. Inoltre, in linea generale, se il legislatore eurounitario tradizionalmente muove dall'esigenza di proteggere gli interessati dai rischi posti dall'utilizzo dell'automazione a fini decisionali[542], il legislatore statunitense muove dall'opposto assunto per cui il carattere automatizzato delle decisioni è garanzia di maggiore precisione, efficienza e neutralità[543].

Ciononostante, la Commissione europea, prendendo espressamente atto del sempre più frequente ricorso, nell'economia digitale, a trattamenti automatizzati come base per l'adozione di decisioni aventi ripercussioni significative sugli interessati, ha disposto l'avvio di "un dialogo sul processo decisionale automatizzato, confrontandosi tra l'altro sulle analogie e sulle differenze d'impostazione tra l'UE e gli USA[544]". Stessa esigenza di approfondimento e monitoraggio è stata poi ribadita in occasione del rapporto sulla prima revisione annuale del funzionamento del *Privacy Shield*[545].

Allo scopo, la Commissione ha curato una ricognizione empirica e giuridica della disciplina sui processi decisionali automatizzati vigente negli Stati Uniti, le cui risultanze, pur limitate dal carattere embrionale e sostanzialmente opaco del fenomeno, hanno messo in evidenza come i settori maggiormente coinvolti siano quelli dell'utilizzo dei dati

[541] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 33.

[542] Nelle parole dell'autrice "[*w*]*hile the person and people of Europe may be legally constituted as entities protected from automated decision-making and deserving of a human in the loop, those in the U.S. are protected from the flaws of humanity through the computational neutrality of information systems*." Così M. LETA JONES, The right to a human in the loop: Political constructions of computer automation and personhood, 47, *Social Studies of Science*, 2, 2017, 216, 231, citata da G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 43.

[543] J.J. RACHLINSKI, S. LYNN JOHNSON, A.J. WISTRICH, C. GUTHRIE, Does unconscious racial bias affect trial judges, 84, *Notre Dame L. Rev*., 2008, 1195. Per la ricostruzione storica del passaggio al *credit scoring* quale rimedio tecnologico agli atteggiamenti discriminatori degli operatori umani si veda J. LAUER, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*, Columbia University Press, NY, 2017.

[544] Scudo UE-USA per la privacy, § 25.

[545] *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU-U.S. Privacy Shield* (COMMISSIONE EUROPEA, Bruxelles, 18 ottobre 2017) (COM (2017) 611 fin.).

sanitari a fini assicurativi ovvero di altri dati sensibili (e potenzialmente discriminatori) a fini di reclutamento lavorativo, nonché dell'utilizzo di informazioni finanziarie a fini di valutazione del merito creditizio della clientela[546].

Il capitolo proseguirà quindi con l'analisi della disciplina vigente in ciascuno di tali settori, non prima però di aver condotto una rapida ricognizione delle principali tappe del percorso di affermazione ed evoluzione del concetto statunitense di privacy e degli ostacoli che lo stesso viene ad affrontare nel contesto digitale. La preliminare ricostruzione dei tratti salienti di quel retaggio giuridico-culturale di cui l'attuale nozione di *data privacy* è espressione risulta, infatti, imprescindibile ad un chiaro inquadramento degli specifici e settoriali interventi legislativi che verranno esaminati nel più ampio contesto del frammentato e multilivello ordinamento degli Stati Uniti. Infine, conclusa la ricognizione del regime giuridico in materia di processi decisionali automatizzati, il capitolo si chiuderà con l'assunzione di una prospettiva di più ampio respiro, volta ad estrapolare dai più recenti sviluppi giurisprudenziali, legislativi e dottrinali indizi della nuova conformazione che il quadro delle fonti di *data privacy* verosimilmente assumerà nel prossimo futuro.

3.2. La matrice dominicale della *proprietary privacy*

Il percorso di affermazione del diritto alla privacy negli Stati Uniti è principalmente giurisprudenziale e legato all'esigenza di limitare l'ingerenza del governo britannico prima, e federale poi, nella vita dei cittadini della neonata federazione nordamericana. È in quest'ottica che si spiega la preponderante attenzione che le concettualizzazioni statunitensi in materia di privacy dedicano al rapporto tra governo federale/statale e cittadini[547]. A tale elaborazione dottrinale e giurisprudenziale viene quindi dedicata la parte introduttiva del paragrafo, essenziale a comprendere il contesto

[546] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 8.

[547] R.J. KROTOSZYNSKI JR, *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford, Oxford University Press, 2016, 16 ss: ID., Back to the Briarpatch: An Argument in Favor of Constitutional Meta-analysis in State Action Determinations, 94, *Mich. L. Rev*., 2, 1995, 302 ss.

socio-culturale, prima ancora che normativo, con il quale si viene a confrontare l'aspirazione extraterritoriale del GDPR.

Come avvenuto nell'Europa continentale oltre un secolo più tardi[548], anche in Nordamerica la privacy nasce innanzitutto in termini di riservatezza verso inopportune ed ingiustificate intrusioni nella vita dei singoli, specialmente in termini di inviolabilità della corrispondenza e della vita familiare. Tracce di attenzione verso esigenze di riservatezza della corrispondenza sono rinvenibili già nel *Post Office Act*, adottato dal Parlamento britannico nel 1710 ed entrato in vigore in Nord America nel 1711. In tale occasione, infatti, si stabilì espressamente come "[*n*]*o Person or Persons shall presume wittingly, willingly or knowingly, to open, detain or delay or cause, procure, permit, or suffer to be opened, detained, or delayed, any Letter or Letters, Packet, or Packets* [549]."

Fu però il formante giurisprudenziale a trasformare questa timida sensibilità in una più ampia e onnicomprensiva nozione di privacy. Analogamente alla scelta compiuta in molti ordinamenti dell'Europa continentale quasi due secoli dopo[550], i cc.dd. *Framers* della Costituzione degli Stati Uniti d'America non riconobbero espressamente il diritto

[548] È noto, infatti, come la prima affermazione legislativa del diritto alla riservatezza sia individuabile nella Dichiarazione Universale dei Diritti dell'Uomo che, nel 1948, all'articolo 12 sancì il diritto di ciascun individuo a non essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della reputazione. Analoga previsione venne poi inclusa nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) firmata a Roma il 4 novembre 1950 che, all'articolo 8, riconobbe il diritto al rispetto della vita privata e familiare. V. CUFFARO, *Profili introduttivi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019, 15 ss; A. PISAPIA, *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli Editore, Torino, 2018, 7ss; G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in ID. (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017, 4 ss; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali: il Regolamento europeo 2016/679*, Giappichelli Editore, Torino, 2016, 27ss.

[549] K. LEIGH, *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 2 ss.

[550] Esula dallo scopo dell'analisi qui condotta richiamare il percorso di affermazione del diritto alla privacy nei vari ordinamenti nazionali del vecchio continente. Basti qui ricordare come le prime legislazioni nazionali a riconoscere espressamente il diritto alla riservatezza in Europa risalgano a interventi di Francia e Germania degli anni '70, mentre la Spagna fu la prima, nel 1978, ad introdurre una espressa previsione nell'articolo 18 della sua Costituzione. In Italia, invece, è noto come nella seconda metà del '900 la Cassazione italiana ancora sostenesse come "un diritto alla riservatezza […] nel senso tipico ritenuto dalla sentenza impugnata non può, in mancanza di esplicita previsione, affermarsi né lo si può ritenere per analogia sulla base di singoli diritti di personalità, dato che singoli concreti aspetti non consentono di precisare un principio che giustifichi il riconoscimento e la efficacia propria di un autonomo diritto soggettivo ad una non precisata riservatezza." Così Cass. civ. 24 aprile 1963 n.990, nonché *ex multis* Cass. 22 maggio 1975 n. 2129 e, prima, Cass. civ., 22 dicembre 1956 n. 4487. Cfr. A. BARBAZZA, *Natura, contenuto e struttura dei diritti della personalità* in S. RUSCICA (a cura di), *I diritti della personalità*, Padova, Cedam, 2013, 60-66; D. VANNI, Protezione dei dati personali (voce), *Digesto*, 2013; G. BUSIA, Diritto alla riservatezza (voce), *Digesto*, 2000.

alla privacy, neppure nella sua più tradizionale declinazione di riservatezza[551]. Ciononostante, non mancarono appigli normativi a supporto di una sua genesi esegetica. Già nel 1878, infatti, la Corte Suprema nel caso *Ex Parte Jackson* ammise come dal combinato disposto del Quarto[552] e Quinto[553] emendamento discendesse una garanzia costituzionale di intangibilità non soltanto verso le mura abitative, ma anche verso la corrispondenza privata[554].

Guardando poi alla crescente invasività delle tecnologie a disposizione dei *Media*, determinante fu l'impulso interpretativo fornito da Louis D. Brandeis e Samuel D. Warren Jr. che per primi, nel loro arcinoto articolo, concettualizzarono il "*right to privacy*"[555]. Ancora più fondamentale, però, fu l'attenzione che Brandeis continuò a mostrare per tale diritto nelle vesti di giudice della Corte Suprema degli Stati Uniti. Uno dei primi capisaldi giurisprudenziali del percorso di affermazione della privacy, infatti, è tradizionalmente individuato nella *dissenting opinion* che lo stesso scrisse in relazione al caso *Olmstead v.*

---

[551] Parzialmente diversa la situazione rispetto alle Costituzioni dei singoli Stati. In California, ad esempio, l'articolo I, sez, I, della Costituzione riconosce che "*all people are by nature free and independent, and have certain inalienable rights, among which are those of* […] *protecting property; and pursuing and obtaining safety, happiness and privacy*". Analoga espressa previsione è rinvenibile nella Costituzione della Lousiana, la quale all'articolo II, sez. 10, riconosce il *right of individual privacy*. Le costituzioni di molti altri Stati, invece, pur non fissando espressamente un tale diritto, riproducono pressoché pedissequamente il disposto del Quarto emendamento. Cfr. W. FREEDMAN, *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987, 89-90.

[552] Tale emendamento dispone "[*t*]*he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*."

[553] In virtù del Quinto emendamento: "[*n*]*o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation*."

[554] È questa la c.d. *conversational privacy*, sottocategoria della *proprietary privacy* (sulla categorizzazione si veda meglio *infra* nel testo) in virtù della quale "*in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution*." Così la Corte Suprema federale in *Ex parte Jackson* (96 U.S. 727, 1878). L'estensione di una sfera di inviolabilità fino a quel momento confinata entro le mura domestiche, per ricomprendevi anche il contenuto di corrispondenza personale, venne poi confermata in *Boyd v U.S.* (116 U.S. 616, 1886) dove la Corte assimilò il sequestro o l'obbligo di produzione di tale documentazione ad una forma di autoincriminazione per mezzo della corrispondenza privata in violazione del Quinto emendamento. Tale principio, in adeguamento all'evoluzione tecnologica, venne poi applicato analogicamente alle nuove tecniche di intercettazione di conversazioni orali in mancanza di valido mandato. Cfr. K. LEIGH, *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 18 ss.

[555] L.D. BRANDEIS e S.D. WARREN JR., The Right to Privacy, 4, *Harv. L. Rev*., 5, 1890, 193ss.

United States (277 US 438, 1928)[556]. Fu questa una delle prime occasioni in cui il Giudice Brandeis ebbe modo di sottolineare come, tra le condizioni strumentali a quel "*pursuit of happiness*" riconosciuto dalla Costituzione degli Stati Uniti fosse annoverabile anche il "diritto ad essere lasciati soli", ricavabile dal Quarto emendamento e implicante l'illegittimità di "*every unjustifiable intrusion by the government upon the privacy of the individual, whatsoever the means employed* [557]."

Siffatta presa di posizione della Corte, oltre alla speciale attenzione al rapporto Stato-cittadino, consente di mettere in evidenza un'altra fondamentale peculiarità della nozione statunitense di privacy che, sebbene in parte superata, continua ad influenzare profondamente l'atteggiamento di giudici e legislatori in materia: la matrice dominicale del diritto. A tal proposito, parte della dottrina ha efficacemente descritto come negli USA il concetto di privacy sia distinguibile in *proprietary privacy* e *decisional privacy*, dove la prima si fonderebbe sulla nozione Lockiana della proprietà, evoluta sino a ricomprendere un diritto di "proprietà" (*rectius* sovranità) sulla propria persona, mentre la seconda muoverebbe dalle teorie sulla libertà di Miller, intesa come controllo sul proprio corpo e sulla propria mente. Nell'accezione proprietaria di privacy vengono ricomprese, fra le altre, questioni concernenti le intercettazioni, il diritto all'immagine e il trattamento dei dati personali a fini sanitari e bancari. Diversamente, controversie vertenti su decisioni di fine vita, sul diritto all'aborto ovvero su unioni fra persone dello stesso sesso, vengono generalmente ricondotte al più generico diritto di privacy decisionale [558]. Più specificatamente, è alle teorizzazioni di Prosser, Gormley, Westin e

[556] Nelle parole della Corte, la c.d. *trespass doctrine* prevedeva che "*for a search to occur, government officials must trespass on private property*." *Olmstead v. United States* (277 US 438, 1928). Cfr. K. LEIGH, *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 22.

[557] In particolare, nelle parole del Giudice "*The makers of* [US] *Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone -the most comprehensive of rights and the right most valued by civilized man. To protect that right every unjustifiable intrusion by the government upon the privacy of the individual, whatsoever the means employed, must be deemed a violation of the Fourth Amendment*." Così L.D. Brandeis, nella sua celebre *dissenting opinion* al caso *Olmstead v. U.S.*, 1928.

[558] M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 12; D.J. SOLOVE, M. ROTENBERG, P. M. SCHWARTZ, *Privacy, Information, and Technology*, New York, Aspen Publishers, 2006, 1.

Allen che risalgono le quattro principali categorizzazioni delle varie declinazioni del diritto.[559]

William Prosser individuò quattro tipologie di c.d. *privacy invasions*, tutte riconducibili a forme di illecito civile[560]: (i) *intrusion upon seclusion* (c.d. *Intrusion Tort*)[561], (ii) *public disclosure of private facts* (c.d. *Private Facts Tort*)[562], (iii) *publicly placing one in a false light* (*False Light Tor*t)[563] e (iv) *appropriation of a person's name*

[559] Cfr. S.T. MARGULIS, *Three Theories of Privacy: An Overview*, in S. TREPTE, L. REINECKE (a cura di), *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer, Berlino, 2011, 9ss.

W. FREEDMAN, *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987, 30-31; M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 3.

[560] W.L. PROSSER, Privacy, 48, *California Law Review*, 3, 1960, 383ss. Cfr. N.M. RICHARDS e D.J. SOLOVE, Prosser's Privacy Law: A Mixed Legacy, 98, *Calif. L. Rev*., 2010, 1887 ss.

[561] Tale sezione, in particolare, statuisce che "*one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another, or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable man*." A titolo meramente esemplificativo, sono riconducibili a tale tipologia di invasione della privacy: intercettazioni illegittime di conversazioni private (*Hamberger v. Eastman*, 206 A2d 239, N.H., 1964); accessi non autorizzati ad informazioni inerenti conti bancari privati (*Zimmerman v. Wilson*, 81 F2d 847, 3rd Cir., 1936); nonché il più classico caso dell'accesso non autorizzato entro il perimetro dell'altrui proprietà privata (i.e. *trespass*), che, come si vedrà meglio *infra* nel testo, è il principale presupposto tradizionalmente utilizzato dalla giurisprudenza per riconoscere una fattispecie di violazione dell'altrui privacy (*ex multis*, *Greeb Valley School, Inc. v. Cowles Florida Broadcasting, Inc*. 327 So2d 810, Fla, 1976). Nello specifico, come chiarito nel caso *Hamberger v. Eastman*, gli elementi costitutivi di tale forma di illecito non presuppone la pubblicazione o la comunicazione a soggetti terzi delle informazioni, anche se una tale circostanza inciderebbe sull'ammontare dei danni liquidati. Cfr. D. SOLOVE e P.M. SCHWARTZ, *Information Privacy Law*, VI ed., Aspen Casebook Series, Wolters Kluwer, New York, 2018, 81 ss.

[562] Si tratta forse dell'ipotesi più affine alla tradizionale nozione di riservatezza, poiché disciplina la pubblicizzazione di fatti fino a quel momento privati, ovvero sui quali il danneggiato vantava una ragionevole aspettativa di privacy, poiché privi di alcuna rilevanza pubblica e quindi non protetti dalla *free speech clause* di cui al Primo emendamento. Inoltre, affinché tale fattispecie sia integrata, la divulgazione dei fatti deve risultare obiettivamente offensiva per l'uomo medio. In particolare, la norma prevede testualmente che "[*o*]*ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public*.". Cfr. W. FREEDMAN, *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987, 45.

[563] La norma stabilisce che "[*o*]*ne who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of privacy, if* (a) *the false light in which the other was placed would be highly offensive to a reasonable person, and* (b) *the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed*" (*ex multis Lord Byron v. Johnston* 35 Eng Rep 851 e *Wood v. Hustler Magazine, Inc*. 744 F.2d 94, 1984). La fattispecie, pur presentando evidenti affinità con la diffamazione, se ne distingue per tre fondamentali elementi: (i) il fatto associato al soggetto leso non deve essere necessariamente falso, ma soltanto fuorviante; (ii) il fatto deve essere particolarmente offensivo o imbarazzante per l'uomo medio, ma non necessariamente dannoso per la sua reputazione; (iii) l'elemento soggettivo del dolo o colpa grave in capo al danneggiante è più attenuato rispetto alla diffamazione, dove tale elevato grado di intenzionalità è richiesto soltanto se il danneggiato è un personaggio pubblico. Cfr. B.R. LASSWELL, In Defense of False Light: Why False Light Must Remain a Viable Course of Action, 34, *Texas Law Review*, 1993, 149 ss; N.E. RAY, Let There Be False Light: Resisting the Growing Trend Towards an Important Tort, 84, *Minn. L. Rev*, 2000, 713 ss. In senso critico D.L. ZIMMERMAN, False Light Invasion of Privacy: The Light That Failed, 64, *N.Y.U. L. rev*., 1989, 364 ss. Per la differenza tra il *False Light Tort* e la diffamazione si veda J. BRESLIN, *False Light: The Tortured and Troubled Tort That Survives*,

or likeness (c.d. *Appropriation Tort*)[564]. Tali quattro tipologie di illeciti civili sono state poi recepite nella tutt'ora vigente disciplina del *Restatement* (*Second*) *of Torts* §652B-E (1977)[565].

Da notare, tuttavia, come siffatto quadro di *tort law* si sia generalmente ritenuto inadeguato a disciplinare il mercato dei dati personali[566]. Il *Tort of Appropriation*[567], ad esempio, è stato ritenuto non applicabile alla vendita del nome del titolare di una carta di pagamento da parte di American Express in quanto, seppure illegittimo, non aveva causato alcuna perdita economica all'interessato[568]. In senso analogo, nel caso *Shibley v. Time, Inc*., i giudici rigettarono l'azione intentata ai sensi dell'*appropriation tort* rispetto alla vendita delle liste dei propri abbonati a società di *direct mail*[569]. Analoga è stata anche la sorte dell'illecito di "*Private Disclosure of Private Facts*" ritenuto inapplicabile al trattamento dei dati di navigazione in rete degli utenti in quanto privo del carattere altamente offensivo richiesto dalla norma che, in tal senso, presuppone la diffusione delle informazioni alla generalità dei consociati[570].

Dal canto suo, optando per una distinzione fondata sulla fonte normativa di tutela, Gormley teorizzò cinque diverse declinazioni della nozione di privacy. In particolare, i quattro illeciti di Prosser vennero tutti raggruppati nella c.d. *Tort Privacy*, distinguendosi poi dalla *Fourth Amendment Privacy*, *First Amendment Privacy*, *fundamental decision privacy* e *state constitutional privacy*[571]. In prospettiva più marcatamente relazionale,

---

in W.A. BABCOCK e W.H. FREIVOGEL (a cura di), *The SAGE Guide to Key Issues in Mass Media Ethics and Law*, Vol. 2, Los Angeles, Sage Publishing, 2015, 527.

[564] Ai sensi della sezione 652C del *Restatement* (*Second*) *of Torts*, tale forma di invasione della privacy opera nel caso in cui "*one who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy*." Tale fattispecie non implica tanto il diritto ad essere lasciati soli in senso stretto, quanto ipotesi di sfruttamento economico dell'immagine altrui senza il consenso dell'interessato. Deciso nel 1905, il caso *Pavesich v. New England Life Insurance Co*. (50 SE 68) è il più risalente esempio di tale forma di illecito. In particolare, la controversia verteva sull'utilizzo del nome, della fotografia e di una fittizia testimonianza dell'attore al fine di pubblicizzare i prodotti assicurativi della convenuta. D.J. SOLOVE, *The Digital Person: Technology and Privacy in the Information Age*, New York, NYU Press, 2004, 60-61.

[565] D.J. SOLOVE, M. ROTENBERG, P. M. SCHWARTZ, *Privacy, Information, and Technology*, New York, Aspen Publishers, 2006, 25 ss.

[566] D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, 114, *Colum. L. Rev*., 2014, 583, 587. Cfr. D.J. SOLOVE, *Understanding Privacy*, Harvard University Press, Cambridge (MA), 2008, 8; N.M. RICHARDS, The Limits of Tort Privacy, 9, *J. on Telecomm. & High Tech. L*., 2011, 357, 365-74.

[567] *Restatement* (*Second*) *of Torts* § 652C.

[568] *Dwyer v. American Express Co*. 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).

[569] 341 N.E.2d 337, 339 (Ohio Ct. App. 1975).

[570] D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 590-591.

[571] K. GORMLEY, One Hundred Years of Privacy, 1992, *Wis. L. Rev*., 5, 1992, 1335ss. Sulle teorizzazioni di Gormley si vedano anche le osservazioni di D. CARPENTER, *Autonomy (of Individuals and*

invece, Westin optò per una quadripartizione in stadi della privacy come solitudine (isolamento fisico), anonimato (*i.e.* assenza di sorveglianza in luoghi pubblici), intimità legata alla dimensione della famiglia o di altre piccole entità di gruppo, nonché come riservatezza, quest'ultima intesa come protezione delle comunicazioni interindividuali e dipendente dalla discrezione di chi ci circonda[572].

Allen, infine, pur muovendo da premesse affini a quelle di Ruth Gavison[573], della privacy come limitazione all'accesso, elaborò una quadruplice classificazione della privacy in termini decisionali, informativi, proprietari e di proprietà privata. La *decisional privacy*, come già accennato, consisterebbe nella libertà di compiere scelte attinenti la sfera più intima e familiare di un individuo e spesso associata al concetto di autonomia o addirittura consideratane il presupposto[574]. La privacy informativa, invece, è la declinazione più affine al concetto europeo di protezione dei dati personali, essendo volta a proteggere gli individui dalla raccolta e diffusione indiscriminata di informazioni personali, così estendendosi, a controversie riguardanti, fra gli altri, dati sanitari, intercettazioni e sorveglianza sulla corrispondenza digitale da parte del datore di lavoro[575]. Da ultimo, la privacy proprietaria è più strettamente collegata al controllo sull'utilizzo del proprio nome e della propria immagine, e si distingue dalla dimensione più fisica della privacy in termini di proprietà privata, riguardata esclusivamente come isolamento individuale[576]. Come accennato in apertura, più recente dottrina ha però opportunamente riunito le ultime tre categorie Alleniane in un'unica più onnicomprensiva

Private Associations), in M. TUSHNET, M.A. GRABER, S.LEVINSON (a cura di), *The Oxford Handbook of the U.S. Constitution*, Oxford, Oxford University Press, 2015, 567.

[572] A. WESTIN, *Privacy and Freedom*, II ed., New York, Ig Publishing, 2015.

[573] R. GAVISON, Privacy and the Limits of Law, 89, *Yale Law Journal*, 1980, 421 ss.

[574] Sul rapporto tra privacy e autodeterminazione si veda anche L. HENKIN, Privacy and Autonomy, 74, *Columbia Law Review*, 7, 1974, 1410 ss.

[575] *Whalen v. Roe* (429 US 589, 1976) è uno dei primi casi in cui venne esplicitamente affrontata la questione della configurabilità di un diritto di proprietà (e quindi un conseguente diritto alla privacy) sulle informazioni al fine di prevenirne la circolazione indiscriminata ed illegittima, specialmente ove raccolte e archiviate con modalità elettroniche. In tale controversia, in particolare, lo Stato di New York aveva adottato una previsione normativa che imponeva la raccolta dei nominativi di tutte le persone che risultavano far uso di droghe quali, fra gli altri, oppiacei, cocaina e anfetamine, sia sulla base di valide prescrizioni mediche che in modo illegale. Tali informazioni venivano registrate su nastri magnetici poi archiviati per cinque anni in una camera blindata protetta da un recinto chiuso a chiave e un sistema di allarme. La Corte ritenne, all'unanimità, che le finalità pubbliche perseguite e le adeguate misure di sicurezza predisposte neutralizzavano qualsivoglia rischio per la privacy dei singoli coinvolti nel programma. Cfr. W. FREEDMAN, *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987, 74.

[576] A. L. ALLEN, *Uneasy Access: Privacy for Women in a Free Society*, Totowa (NJ), Rowman & Littlefield, 1988.

nozione di privacy proprietaria, inglobante tutte situazioni in cui il diritto alla privacy viene riconosciuto in capo a chi dimostra di vantare una posizione dominicale, seppure su oggetti immateriali come la propria immagine o le proprie informazioni personali[577].

Da notare, tuttavia, che la matrice Lockiana della nozione di proprietà ivi richiamata è volta non a tanto a individuare un regime giuridico per la circolazione di dati personali, quanto, ancora una volta, a rimarcare una linea netta di confine tra la sfera pubblica e la sfera privata, oltre la quale al governo (inteso in senso lato di potere pubblico, sia esso giurisdizionale, politico o amministrativo) non è costituzionalmente consentito di muoversi[578].

È proprio questa matrice dominicale, bene espressa nel sopracitato caso Olmstead, che ha reso per lungo tempo impossibile estendere la protezione del Quarto emendamento ad aspetti della vita più immateriali, come le conversazioni o la vita familiare in senso lato.

3.3. Il Katz test: per una privacy delle persone e non dei luoghi

La tradizionale e restrittiva concezione proprietaria della privacy inizia a vacillare nel 1965, quando in occasione del caso *Griswold v. Connecticut* la Corte Suprema riconobbe, per la prima volta, l'esistenza di una base costituzionale per il diritto alla privacy[579]. In particolare, nel dichiarare l'illegittimità costituzionale di una legge del Connecticut che impediva l'utilizzo di farmaci per finalità contraccettive, il giudice Douglas, scrivendo per la maggioranza, elaborò quello che divenne noto come il c.d. *penumbra argument*. Nelle parole del giudice, infatti, sebbene i padri fondatori non

[577] M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 3.

[578] Si ricorda, infatti, come le teorizzazioni di Locke fossero finalisticamente orientate a contrastare posizioni di chi, come Robert Filmer, avanzava e sosteneva l'idea di un potere paternalistico e quindi assoluto del monarca sui suoi sudditi. È così nel tentativo di contrastare queste insinuazioni che Locke sviluppa l'idea di un uomo "*master of himself, and proprietor of his own person, and the actions or labour of it, had still in himself the great foundation of property*". J. LOCKE, *Second Treaties of Government*, 1690, 19. Cfr. M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 22ss; P. LASLETT, *Patriarcha and other political works of Sir Robert Filmer*, Oxford, B. Blackwell, 1949.

[579] Più specificamente, il caso prese le mosse dalle accuse di favoreggiamento mosse nei confronti di Estelle Griswold, direttore esecutivo della *Planned Parenthood League* del Connecticut, organizzazione alle frontiere della lotta per il diritto all'autodeterminazione femminile sul proprio corpo, specialmente a livello procreativo. *Griswold v. Connecticut* (381 U.S. 479, 1965).

avessero espressamente menzionato il diritto alla privacy in nessun emendamento, questo cionondimeno esisterebbe nel cono d'ombra generato dal primo, terzo, quarto, quinto, nono e quattordicesimo emendamento[580].

È peraltro in questa decisione che venne piantato il seme di quel diverso ramo statunitense del diritto alla privacy che, dopo aver finalmente ottenuto dignità costituzionale, iniziò a guardare oltre il Quarto emendamento. In particolare, come osservato dal giudice Goldberg nella sua *concurring opinion* (condivisa anche dai giudici Warren e Brennan): con l'introduzione del Nono emendamento si volle aprire un varco nel muro di recinzione che fino a quel momento aveva rigidamente perimetrato la sfera del costituzionalmente rilevante, offrendo tutela anche a situazioni giuridiche non espressamente prese in considerazione nel *Bill of Rights*[581].

A dispetto delle innegabili sfumature personalistiche assunte dalla nozione statunitense di privacy per effetto della giurisprudenza inaugurata con Griswold, il retaggio proprietario dell'*informational privacy* venne puntualmente affrontato soltanto nel 1967, quando la Corte suprema si trovò a decidere il noto caso *Katz v. U.S.* (389 U.S. 347, 1967)[582].

La controversia prese le mosse dalle accuse avanzate contro il Sig. Charles Katz: un allibratore sospettato di essersi avvalso di una cabina telefonica pubblica per organizzare e raccogliere scommesse illegali. Nonostante l'apparente banalità della lite, della stessa venne investita la Corte Suprema che si ritrovò così a dover sciogliere la non altrettanto banale questione del livello di riservatezza da riconoscere a tale modalità di

[580] Più puntualmente: "*The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers 'in any house' in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'. The Fifth Amendment, in its Self-Incrimination Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: 'The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people'. The Fourth and Fifth Amendments were described in* Boyd v. United States, *116 U.S. 616, 630, as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life'."* Così il Giudice Douglas in *Griswold v. Connecticut* (381 U.S. 479, 1965), 484.

[581] Cfr. K.L. HALL e J.J. PATRICK, *The Pursuit of Justice. Supreme Court Decisions that Shaped America*, Oxford, Oxford University Press, 2006, 152.

[582] Cfr. P. FINKELMAN, *The Encyclopedia of American Civil Liberties: A - F, Index*, New York, Routledge, 2006, 1220 ss.

conversazione. Nel caso di specie, infatti, la *Federal Bureau of Investigation* (FBI) aveva posizionato dei microfoni presso una delle due cabine telefoniche normalmente utilizzate dal Sig. Katz, rendendo fuori servizio l'altra. I microfoni, tuttavia, erano stati collocati all'esterno della cabina telefonica, in modo tale da consentire all'FBI di ottenere le registrazioni delle conversazioni ivi tenute dall'indagato senza che lo spazio interno della cabina fosse fisicamente "invaso". Questa circostanza, in virtù della *trespass doctrine* utilizzata in Olmstead avrebbe, secondo gli agenti governativi, precluso la configurabilità di una violazione del diritto alla privacy dell'interessato.

Al contrario, nello scrivere per la maggioranza, il giudice Potter Stewart coniò il celebre principio per cui "*the Fourth Amendment protects people, not places*[583]*."* Nel caso di specie, quindi, sebbene il Governo avesse argomentato che la natura pubblica e la costruzione in vetro della cabina avrebbero dovuto precludere la legittimità di una qualsivoglia aspettativa di riservatezza da parte dell'indagato, la Corte ritenne che il Sig. Katz nell'entrare nella cabina e chiudere la porta alle sue spalle avesse ragionevolmente creduto di escludere l'orecchio, non lo sguardo altrui[584]. Per questo motivo, la Corte concluse che la circostanza per cui i dispositivi di registrazione non avessero infranto le barriere fisiche della cabina telefonica fosse costituzionalmente irrilevante. Fu qui, quindi, che la giurisprudenza statunitense compì il passo ermeneutico necessario a svincolare la tutela della privacy dalla "*trespass doctrine*", inaugurando la stagione della "*privacy doctrine*". Ciò non significa, tuttavia, che la variabile proprietaria venne completamente eliminata dall'equazione della privacy, ma che, più limitatamente, la formula venne arricchita con altri elementi, in modo tale da poter estendere la sfera di riservatezza dei cittadini al di fuori delle mura domestiche[585].

[583] Chiarisce il Giudice: *"[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of the Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected*." *Katz v. U.S.* (389 U.S. 347, 1967), 351. Cfr. M. MOSKOVITZ, *Cases and Problems in Criminal Procedure: The Police*, V ed., LexisNexis, 2010, 142 ss.

[584] J. SAMAHA, *Criminal Procedure*, X ed., Belmont (CA), Wadsworth, 2018, 55 ss.

[585] In questo senso, in dottrina si fa notare come il Katz test non rappresenti un vero e proprio passaggio dalla proprietà alla privacy, ma piuttosto un tentativo di introdurre un nuovo criterio interpretativo di applicazione della tutela del Quarto emendamento che potesse rispondere con maggiore sensibilità alle esigenze poste dall'evoluzione tecnologica, senza svalutare del tutto gli altri precedenti giurisprudenziali. Si crea così una linea di rottura che, guardando al futuro, consente di preservare la validità degli insegnamenti del passato. O.S. KERR, The Curious History of Fourth Amendment Searches, 2012, *The Supreme Court Review*, 2012, 67 ss.

Nel chiarire la portata applicativa dell'assunto così introdotto, il giudice Marshall Harlan redisse la *concurring opinion* fonte di quella tecnica di verifica giurisprudenziale di esistenza dei presupposti operativi della *privacy doctrine*, tutt'ora utilizzata e incentrata sul concetto della "*reasonable expectation of privacy*"[586]. In particolare, il test si configura come duplice: da un lato, la persona interessata deve aver mostrato una concreta aspettativa di riservatezza (elemento soggettivo); dall'altro, la società deve essere pronta a riconoscere tale aspettativa come ragionevole (elemento oggettivo)[587]. Per tal via, le osservazioni anni prima criticamente avanzate da Brandeis in Olmstead, e qui recepite, divennero finalmente parte integrante della "*law of the land*"[588].

3.4. La (non) ragionevolezza dell'aspettativa di privacy nella rete

Prima di procedere all'analisi degli interventi legislativi che hanno progressivamente integrato e arricchito la disciplina della privacy, specialmente con riguardo alla comprensibilità dei processi decisionali, è necessario concludere questa preliminare ricognizione giurisprudenziale definendo più puntualmente i confini interpretativi entro i quali l'aspettativa di riservatezza fin qui analizzata viene tradizionalmente considerata ragionevole.

La connotazione soggettiva e relativa di tale presupposto di protezione della privacy, infatti, rende inevitabile chiedersi in che misura l'attuale regime di condivisione e circolazione delle informazioni in rete possa limitare la possibilità dei giudici statunitensi di riconoscere, anche nel contesto digitale, una ragionevole aspettativa di privacy. Come efficacemente osservato, infatti, "[*t*]*he Fourth Amendment contains what Justice Brandeis describes as a right to keep thoughts and ideas private from a prying world. But what happens when many of those previously private thoughts are displayed on social media for the world to see*?[589]*.*"

[586] *Katz v. U.S.* (389 U.S. 347, 1967), 361.

[587] M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 52-53.

[588] J. SAMAHA, *Criminal Procedure*, X ed., Belmont (CA), Wadsworth, 2018, 55 ss.

[589] R. PRUNTY e A. SWARTZENDRUBER, *Social Media and the Fouth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 400. Cfr. L.S. FEUER, Who is Poking Around Your Facebook Profile? The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites, 40, *Hofstra Law Review*, 2, 2011, 473ss.

In particolare, il richiamato percorso ermeneutico di affermazione della *privacy doctrine* ha parallelamente stimolato riflessioni sui limiti della stessa, tradizionalmente individuati nelle teorie della "*plain-sight*" e della "*third-party*" (anche nota come "*misplaced confidence*").

Tali eccezioni, accomunate dall'escludere la protezione del Quarto Emendamento verso azioni governative volte ad ottenere informazioni già uscite dalla sfera di riservatezza (*rectius* controllo esclusivo) dell'interessato, sollevano però interrogativi peculiari e spesso irrisolti nel contesto digitale.

3.4.1. La plain-sight doctrine come limite alla riservatezza di informazioni archiviate sul proprio personal computer

La *plain-sight doctrine* è un'eccezione all'applicabilità della protezione di cui al Quarto emendamento in virtù della quale ove agenti di polizia, nel condurre le loro ordinarie attività di indagine e perquisizione, rinvengano materiale probatorio relativo ad altri reati "in piena vista" possono sequestrarlo anche in assenza di uno specifico mandato[590]. La dottrina ha risalenti radici di *common law* e, ancora una volta, mostra profondi (seppur non immediatamente evidenti) legami con la *trespass doctrine* e, quindi, con la matrice dominicale del diritto alla privacy. Tale affinità emerge chiaramente nelle parole di Lord Camden, per cui "*the eye cannot by the laws of England be guilty of a trespass*[591]*."* La *ratio* giustificatrice dell'eccezione risiede nell'esigenza di prevenire la distruzione di materiale probatorio, specialmente nel caso in cui l'interessato, avendolo lasciato "in piena vista", non possa più vantare su di esso una legittima aspettativa di riservatezza[592].

[590] D. SCHULTZ e J.R. VILE, *The Encyclopedia of Civil Liberties in America*, New York, Routledge, 2015, 709; M.E. LEONARD, *The Chainging Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 314.

[591] *Entick v. Carrington*, 19 Howell's State Trials 1029 (1765). M.A. GRABER e H. GILLMAN, *The Complete American Constitutionalism. Introduction and the Colonial Era*, Vol. I, Oxford, Oxford University Press, 2015, 488-489. Cfr. T.N. MCINNIS, *The Evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 94.

[592] Ad esempio, nel caso *Florida v. Riley* (488 U.S. 455, 1989) la Corte Suprema negò la configurabilità di una legittima aspettativa di privacy su aree di proprietà privata costituite da campi aperti. In particolare, nel caso di specie il Sig. Riley era stato condannato per produzione di sostanze stupefacenti dopo che un'agente di polizia, sorvolando in elicottero il suo terreno, aveva notato l'esistenza di coltivazioni sospette, e aveva quindi ottenuto un mandato. Contestata la condanna perché fondata su prove ottenute in presunta violazione del Quarto emendamento, la Corte Suprema ritenne che, nella misura in cui, da un lato, chiunque avrebbe potuto sorvolare legalmente sul terreno e, dall'altro, tale attività non aveva interferito con il godimento della proprietà, l'azione compiuta dall'agente prima di ottenere il mandato non integrava gli

Allo stesso tempo, tuttavia, al fine di evitare che tale teorizzazione potesse essere utilizzata per legittimare cc.dd. *exploratory searches*, il giudice Stewart, in una serie di opinioni scritte in occasione del caso *Coolidge v. New Hampshire* (403 U.S. 443, 1971)[593], chiarì che l'operatività di siffatta eccezione avrebbe dovuto essere sottoposta ad un triplice ordine di limitazioni[594]. In primo luogo, l'agente di polizia non può avvalersi dell'eccezione per iniziare una perquisizione *ex novo*, ma deve mostrare il diverso motivo che ha legittimato il suo accesso allo spazio in cui viene condotta la ricerca. In secondo luogo, la deroga opera solo rispetto alla scoperta di oggetti che, pur non rientrando nello scopo del mandato, non hanno richiesto ulteriori attività, essendo stati rinvenuti accidentalmente nello svolgimento delle legittime operazioni di perquisizione[595]. Da ultimo, il carattere incriminante di tale materiale probatorio deve risultare evidente ad "un primo sguardo", non essendo consentita alcuna forma di contatto con lo stesso[596].

---

estremi di una "*search*" e quindi l'interessato non poteva vantare una ragionevole aspettativa di privacy sul terreno. Cfr. H.G. WOLF, *Drones. Safety Risk Management for the Next Evolution of Flight*, New York, Routledge, 2017, 140 ss.

[593] Il caso prendeva le mosse dalle indagini per l'omicidio della quattordicenne Pamela Mason, per il quale il Sig. Coolidge era indagato. Nello svolgere le indagini, gli agenti chiesero e ottennero un mandato per procedere al sequestro del veicolo dello stesso. Tale autorizzazione venne poi dichiarata invalida, dando modo alla Corte Suprema di pronunciarsi sui limiti della *plain-sight doctrine*. T. MACLIN, *The Supreme Court and the Fourth Amendment's Exclusionary Rule*, Oxford, Oxford University Press, 2013, 136 ss.

[594] In particolare, fu in tale occasione che la Corte ebbe modo di chiarire come la *plain-sight doctrine* fosse compatibile con entrambe le funzioni base del Quarto Emendamento: assicurare che le perquisizioni siano condotte solo in presenza di una c.d. "*probable cause*" e impedire alle forze dell'ordine di condurre ricerche non sufficientemente circoscritte ad una determinata ipotesi di reato o alla ricerca di specifici elementi di prova.

[595] Sebbene il carattere "accidentale" della scoperta sia stato progressivamente abbandonato, come precisato dal Giudice Stevens in *Horton v. California* (496 U.S. 128, 1990), l'operatività della dottrina continua ad implicare un triplice test volto a determinare: (i) se il materiale probatorio era in "piena vista"; (ii) se il carattere incriminante dell'oggetto era di immediata evidenza e, da ultimo, (iii) se l'agente di polizia poteva legittimamente acquisire il possesso dello stesso. Nel caso in esame, ad esempio, la Corte ritenne legittimo il sequestro di armi trovate nell'abitazione di un indagato per rapina, anche se il mandato aveva espressamente autorizzato la ricerca dei soli proventi del diverso reato oggetto d'indagine. M.E. LEONARD, *The Changing Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 404-405.

[596] Ad esempio, nel caso *Texas v. Brown* (460 U.S. 730, 1983) la Corte ritenne che tale presupposto non fosse stato violato nel caso in cui un agente di polizia avesse provveduto a spostare un veicolo parcheggiato in luogo pubblico per meglio ispezionarlo. In tal senso, i giudici conclusero quindi che l'interessato non possa vantare una legittima aspettativa di privacy sull'esterno di un veicolo, se sostato in luogo liberamente accessibile al pubblico. In senso analogo, nel caso *Arizona v. Hicks* (480 U.S. 321, 1987) la Corte Suprema precisò che lo spostamento di apparecchiature radiofoniche per prendere nota del numero di serie al fine di verificare se fossero o meno proventi di un reato diverso da quello che aveva giustificato l'inizio delle operazioni di perquisizione esulasse dall'ambito di operatività della *plain-sight doctrine*. Più specificatamente, il Giudice Scalia nello scrivere per la maggioranza precisò che "[*t]he distinction between 'looking' at a suspicious object in plain view and 'moving' it even a inches is much more than trivial for purposes of the Fourth Amendment. It matters not that the search uncovered nothing of any great personal value to respondent -serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs. A search is a search, even if it happens to disclose nothing but the*

Calando la fattispecie nel contesto digitale, non possono non sorgere peculiari perplessità concernenti il rischio che tale esonero possa aggravare la già marcata invasività di indagini compiute tramite ricerche di materiale probatorio digitale archiviato su *personal computer*s[597]. Innanzitutto, incertezze sorgono rispetto all'individuazione di tecniche ermeneutiche attraverso le quali la *plain-sight doctrine*, originariamente concepita con riguardo a spazi fisici, possa essere adattata a ricerche in spazi virtuali[598]. A tal fine, tre sono i principali approcci adottati in contesti digitali dalle Corti statunitensi.

Il primo è quello noto come *inadvertent approach*, per effetto del quale il materiale probatorio relativo al reato B ricercato dagli agenti dopo averne inavvertitamente individuato un primo elemento nel corso di indagini relative al diverso reato A, è inutilizzabile nel processo poi avviato rispetto al capo d'imputazione B[599]. Una seconda e più radicale declinazione ermeneutica della dottrina, invece, incentrandosi sul c.d. *prophylactic test*, ne vieta totalmente l'applicazione al mondo virtuale. In virtù di tale approccio, quindi, la perquisizione di materiale probatorio digitale contenuto in un computer è ammissibile solo se supportata da uno specifico mandato che autorizzi ricerche legate a puntuali ipotesi di reato. Nel caso *United States v. Comprehensive Drug Testing, Inc*., ad esempio, la Corte impose il coinvolgimento di tecnici specializzati (cc.dd. *filter teams*) i quali avrebbero dovuto trasmettere al *prosecutor* e ai giudici i soli dati pertinenti al capo d'imputazione, stralciando e restituendo al proprietario ogni altro *file*[600]. L'ultima, e più diffusa, impostazione interpretativa è però quella improntata al c.d. *computer-as-container approach* in base al quale le perquisizioni di documenti

bottom of a turntable." Cfr. T.N. MCINNIS, *The Evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010, 95-96.

[597] M.E. LEONARD, *The Changing Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 312.

[598] W.J. ROBINSON, Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act, 98, *Georgetown Law Journal*, 4, 2010, 1163 ss; R. PRUNTY e A. SWARTZENDRUBER, *Social Media and the Fourth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 413.

[599] Così la Corte in *United States v. Carey* (US Court of Appeal, 10th Cir, 1999) dove i giudici ritennero che le immagini pedopornografiche casualmente trovate sul computer dell'indagato, nel corso di ricerche sullo stesso autorizzate da mandato per il diverso reato di traffico di stupefacenti, fossero inutilizzabili. In particolare, l'agente di polizia, dopo aver accidentalmente individuato un'immagine, aveva intenzionalmente proseguito le ricerche in tale direzione, nel tentativo di ricercare ulteriore materiale analogo. Cfr. E. BAXTER JR., *Complete Crime Scene Investigation Handbook*, Boca Raton (FL), CRC Press-Taylor and Francis Group, 2015, 23 ss.

[600] Così *United States v. Comprehensive Drug Testing, Inc*. (621 F. 3d 1162 9th Cir, 2010). Il caso muoveva da indagini per doping avviate per il sospetto che un gruppo di giocatori professionisti di baseball avesse fatto uso di steroidi. Cfr. A.G. PARISI, *E-contract e privacy*, Torino, Giappichelli Editore, 2015, 55.

digitali dovrebbero essere in tutto e per tutto equiparate a quelle aventi ad oggetto materiale analogico-cartaceo. Il computer, in questo senso, viene assimilato ad un cassetto contenente documenti. Ciò in quanto, sostiene la dottrina maggioritaria[601], le tradizionali garanzie insite nel Quarto emendamento sarebbero di per sé sufficienti a prevenire ricerche eccessivamente ampie, a prescindere dal mezzo tecnologico utilizzato[602]. Al contrario, non manca chi, come Behar, ritiene che la quantità, varietà e, in ultima analisi, pervasività, delle informazioni potenzialmente archiviabili (e generalmente archiviate) in un computer rendono inadeguata la semplice estensione analogica delle teorizzazioni sinora elaborate con riguardo al mondo materiale. Nelle parole dell'Autore, infatti, in tal modo si consentirebbe al governo di ottenere "*a snap shot of the citizenry's private life*".[603]

Sono proprio questi timori che, aggravati dall'assenza di una pronuncia della Corte Suprema o di una legislazione specifica sul punto, hanno spinto parte della dottrina e della giurisprudenza ad individuare soluzioni diverse e più sensibili allo specifico contesto tecnologico di riferimento.

Un primo rimedio individuato da parte della dottrina sarebbe quello di assimilare l'accesso alle informazioni disseminate ed archiviate in formato digitale (perlomeno se archiviate in *Cloud* o *hardware* personali) al principio applicato in *Riley v. California* (573 U.S. 373, 2014). In tale caso, infatti, la Corte Suprema ritenne che la perquisizione del telefono cellulare trovato indosso al soggetto arrestato, in assenza di mandato, costituisse una violazione del Quarto emendamento. Sebbene la dottrina della "*search-incident-to-arrest*" (c.d. SITA *doctrine*) consenta, in linea generale, una tale ispezione, questa non può legittimamente estendersi alle informazioni raccolte in un cellulare. Ciò, innanzitutto, in ragione della specifica *ratio* sottesa alla dottrina: dare alle forze

[601] In questo senso, ad esempio, C.J. MANTEI, Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches, 53, *Ariz. L. Rev*., 2011, 985 ss; K. BRUEGGEMANN WARD, The Plain (or Not So Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures, 79, *University of Cincinnati Law Review*, 3, 2011, 1163ss. Cfr. R. PRUNTY e A. SWARTZENDRUBER, *Social Media and the Fourth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 414; D.J. ZIFF, Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant, 105 *Colum. L. Rev*., 2005, 841ss; O.S. KERR, Fourth Amendment Seizures of Computer Data, 119 *Yale L.J.*, 2010, 700ss.

[602] *Ex multis United States v. Williams* (553 US 285, 2008).

[603] D.C. BEHAR, An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context, 66, *U. Miami L. Rev*., 2012, 471 ss.

dell'ordine la possibilità di sottrarre all'arrestato qualsiasi oggetto suscettibile di essere utilizzato come un'arma. Tale preoccupazione, evidentemente, pur potendo in astratto valere per il dispositivo fisico dell'apparecchio elettronico, di certo non può estendersi ai dati in esso salvati. Inoltre, e forse principalmente, tale esclusione si rende necessaria in ragione del peculiare grado di intimità delle informazioni raccolte in un cellulare. Come acutamente notato dal Giudice Roberts, infatti, "[*m*]*odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought*[604]*"*.

In alternativa, un'altra opzione ermeneutica potrebbe essere quella di applicare il principio di diritto affermato in *Kyllo v. United States* (533 U.S. 27, 2001). In tale occasione, nell'ambito di indagini volte a raccogliere materiale probatorio a supporto del sospetto che il Sig. Kyllo stesse coltivando sostanze stupefacenti nella sua abitazione, gli agenti del dipartimento degli interni degli Stati Uniti si avvalsero di strumenti di rilevazione a distanza di fonti di calore idonei a rilevare la presenza dei particolari dispositivi di illuminazione necessari a sostenere una tale coltura in spazi chiusi. Dopo aver tentato infruttuosamente di far escludere le prove così ottenute, Kyllo dapprima si dichiarò colpevole e poi appellò la sentenza che giunse così alla Corte Suprema. Quest'ultima, seppure con una scarsa maggioranza, ritenne che l'operazione condotta dagli agenti governativi costituisse una invasione della legittima aspettativa di privacy del sospettato. Ciò che, ai fini delle considerazioni sin qui svolte, merita particolare attenzione è lo specifico fattore che indusse la Corte a raggiungere una tale conclusione. I giudici ritennero, infatti, che l'aspettativa di riservatezza avanzata dall'interessato fosse ragionevole, e che quindi le garanzie di cui al Quarto emendamento fossero state violate, in virtù del carattere altamente sofisticato e non generalmente accessibile delle tecnologie utilizzate dagli agenti[605].

[604] *Riley v. California* (573 U.S. 373, 2014), 28. Tale opinione è condivisa in dottrina da chi, richiamando le parole di Roberts, ha sottolineato come "*individual's expectation to privacy is also much higher with digital data stored on a smartphone* […]. *Smartphones differ fundamentally from other objects carried by a person. Although they are tools that might be used to conduct illegal activity, they are much more than that since they* […] *maintain a digital record of nearly every aspect of one's life*." Così J.C. DOMINO, *Civil Rights and Liberties in the 21st Century*, IV ed., New York, Routledge, 2018, 213 ss.

[605] In altre parole, è stato efficamente osservato come "*[p]olice can see and hear the things that any member of the public might see and hear, without fear of Fourth Amendment regulation. Only when*

Si potrebbe, quindi, per tal via tentare di escludere la legittimità costituzionale di indagini compiute in assenza di mandato avvalendosi delle nuove tecniche di *Data Mining* e, più in generale, di *Knowledge Discovery in Databases.* Tuttavia, il sempre più diffuso utilizzo di tali tecniche di analisi dei dati per finalità di *marketing* e il carattere generalmente noto di tali operazioni, seppure non propriamente accessibile, rende particolarmente impervia l'adozione di siffatto percorso ermeneutico. Peraltro, pur volendo ammettere che le informazioni spontaneamente digitalizzate e/o disseminate in rete dagli utenti non siano qualificabili come "in piena vista", la ragionevolezza dell'aspettativa di privacy sulle stesse è cionondimeno compromessa dal secondo limite interpretativo al Quarto emendamento: la c.d. *Third-party doctrine*.

3.4.2. La Third-Party Doctrine come limite alla riservatezza delle informazioni gestite da Internet Service Providers

Per effetto della c.d. *third-party doctrine* (anche nota come *misplaced confidence doctrine*[606]*)* la tutela del Quarto emendamento cade rispetto ad informazioni che sono state volontariamente condivise dall'interessato con soggetti terzi, pur se nella convinzione che l'altra parte fosse vincolata ad un regime di riservatezza o di utilizzo limitato dell'informazione[607]. Nelle parole efficacemente utilizzate dalla Corte nel caso *U.S. v. DeVore* (423 F.2d 1069 4th Cir, 1970): "[*w*]*hen a defendant has a conversation with another person he relinquishes his right of privacy with respect to that person*[608]*."*

they see and hear things that members of the public would not be allowed to see and hear, has a 'search' taken place." Così W. STUNTZ, *Search and Seizure*, in J. DRESSLER (a cura di), *Encyclopedia of Crime & Justice*, II ed., New York, Macmillan Reference USA, 2002, 1387 ss. Cfr. J. SAMAHA, *Criminal Procedure*, X ed., Belmont (CA), Wadsworth, 2018, 57.

[606] J.R. KANOVITZ, *Consitutional Law for Criminal Justice*, XIV ed., New York, Routledge, 2015, 286. Cfr. Note, If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine, 130, *Harv. L. Rev*., 7, 2017, 1924 ss; D.J. SOLOVE, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75, *S. Cal. L. Rev*., 2002, 1083ss.

[607] *Ex multis*, si veda *United States v. Miller* (425 US 435, 1976). In tale caso, il Sig. Mitch Miller era stato accusato e condannato per essere stato colto nell'atto di trasportare materiale per la distillazione di alcool sul quale non erano state pagate le relative tasse. Appellata la sentenza, la Corte ribaltò il verdetto ritenendo che la documentazione bancaria sulla base della quale Miller era stato condannato, era stata ottenuta in violazione del Quarto emendamento. La Corte Suprema, in persona del Giudice Powell, che scrisse per la maggioranza, stabilì che in realtà la documentazione bancaria non è assimilabile alla corrispondenza privata e che, in particolare, non poteva ritenersi invasa la privacy di un individuo nel momento in cui una terza parte, a cui questi aveva volontariamente trasmesso le informazioni, le avesse poi condivise con le forze dell'ordine che hanno fatto richiesta.

[608] La Corte continuò poi precisando che, in tali circostanze, l'interessato "*may constitutionally complain of breach of privacy by an eavesdropper, but not of a breach of trust by the person he chooses to trust, however unwisely. Since the participants in a conversation are privileged to tell what was said, it*

Come la *plain-sight doctrine*, anche questa seconda deroga produce importanti conseguenze nel contesto digitale. Nel caso *United States v. Bynum* (604 F.3d 161, 2010), ad esempio, i giudici esclusero la configurabilità di una ragionevole aspettativa di privacy sulle informazioni che un utente aveva volontariamente fornito ad un *Internet Service Provider*, in questo caso Yahoo![609]. Anche in ambito lavorativo, la Corte Suprema ha avuto modo di chiarire che i dipendenti non possono vantare una ragionevole aspettativa di riservatezza sulle comunicazioni effettuate per mezzo dei dispositivi elettronici messi a disposizione dal datore di lavoro. Ad esempio, nel caso *Ontario v. Quon* (560 U.S. 746, 2010), la Corte Suprema, in persona del giudice Kennedy, che scrisse per la maggioranza, ritenne che, nell'incertezza relativa allo standard sociale in quel momento prevalente rispetto al livello di riservatezza generalmente associato a dispositivi elettronici aziendali, fosse preferibile adottare un'interpretazione ristretta alle specifiche circostanze del caso, sancendo così la legittimità della perquisizione operata dal datore di lavoro sui messaggi scambiati dai dipendenti con *pagers* aziendali[610].

La difficoltà di adattare la *third-party doctrine* all'evoluzione del contesto tecnologico di riferimento è una costante della giurisprudenza in materia e che, tradizionalmente, trova uno dei suoi più classici pilastri interpretativi nel caso *Smith v. Maryland* (442 U.S. 735, 1979). In tale occasione la Corte Suprema si trovò a dover valutare la legittimità dell'aspettativa di privacy paventata dal Sig. Smith sui numeri di telefono digitati. Il giudice Blackmun, nello scrivere per la maggioranza, ritenne che l'utilizzo di un dispositivo di registrazione di numeri composti (c.d. *pen register*) non

necessarily must follow that a recording of what was said may either be used to corroborate the revelation, or simply as a more accurate means of disclosure." *U.S. v. DeVore* (423 F.2d 1069 4th Cir, 1970), 1074. Analogo principio era stato precedentemente affermato anche *in Hoffa v. United States*, (385 U.S. 293, 87, 1966), dove un informatore aveva ingannevolmente ottenuto accesso alla stanza d'hotel dell'indagato, ascoltandone la conversazione di cui poi diede testimonianza. Nello stesso senso anche *Lopez v. United States* (373 U.S. 427, 1963), in cui un agente governativo aveva registrato una conversazione avuta con l'indagato. Cfr. M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 59; J.R. KANOVITZ, *Consitutional Law for Criminal Justice*, XIV ed., New York, Routledge, 2015, 663.

[609] Nel caso di specie, l'FBI aveva richiesto e ottenuto da Yahoo! i dati forniti in fase di registrazione dal Sig. Bynum, indagato per pedopornografia.

[610] Con più specifico riferimento al settore privato, invece, si vedano le analoghe conclusioni raggiunte dalla giurisprudenza in *TBG Insurance Services v. Superior Court* (96 C.A.4th 443, 2002). In tale caso un dipendente, che aveva sottoscritto le policies di utilizzo di due computer messigli a disposizione dal datore di lavoro, in cui espressamente veniva informato del monitoraggio delle attività compiute con tali dispositivi, venne licenziato per inadeguato utilizzo degli stessi. A tal proposito, la Corte ritenne che proprio in virtù del consenso prestato, il dipendente non poteva vantare alcuna ragionevole aspettativa di privacy sulle informazioni contenute nei computers aziendali. Cfr. W. OVERBECK, G. BELMAS, J. SHEPARD, *Major Principles of Media Law*, Cengage Learning, 2017, 237.

richiedesse il previo rilascio di un mandato. Ciò in quanto, gli utenti di un servizio di telecomunicazione sono, o dovrebbero essere, generalmente consapevoli che i numeri composti verranno registrati dalla compagnia telefonica, tanto al fine di consentire l'effettuazione di chiamate, quanto per la necessità di assicurare un corretto addebito dei costi in capo alla clientela. Tale conclusione, in altre parole, sembrerebbe giustificata sia dalla ridotta intimità delle informazioni intercettate, che dal loro carattere strumentale all'erogazione del servizio telefonico[611]. Analoghe considerazioni sono state poi estese, seppure non univocamente[612], ad ipotesi di geolocalizzazione a mezzo tracciamento delle celle telefoniche, escludendo la configurabilità di una violazione della privacy[613].

In particolare, nel caso *United States v. Skinner* (690 F.3d 772 6th Cir., 2012) la Corte statuì che il Sig. Skinner "*did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone* […] *just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car's paint*[614]*."* Lo sfruttamento delle capacità di geolocalizzazione caratterizzanti i telefoni di nuova generazione, proseguì la Corte, non può essere precluso alle forze di

[611] Da notare, tuttavia, che sebbene la registrazione dei numeri telefonici digitati dalla clientela possa costituire un'operazione necessaria ai fini di una corretta fatturazione dei costi da addebitare, non si può dire lo stesso per la registrazione delle conversazioni. Tale operazione, al contrario, ammonta ad una attività di sorveglianza assimilabile alle intercettazioni e quindi illegittima in assenza di mandato. Siffatta considerazione si lega a quella particolare deroga alla tutela della privacy costituita dalla c.d. *business exception* in base alla quale, da un lato, non si può configurare un'invasione della privacy nella misura in cui la raccolta di informazioni rientri nelle abituali e necessarie attività imprenditoriali; mentre, dall'altro, non si può negare al datore di lavoro la possibilità monitorare le conversazioni e la corrispondenza dei propri dipendenti. In particolare, ad esempio, nel caso *DiPiazza v. U.S.* (415 F.2d 99, 1969), poi richiamato in *Nolan v. U.S.* (423 F. 2d 1031, 1969), la Corte chiarì come la registrazione dei numeri di telefono digitati dai clienti (ma non delle loro conversazioni) da parte della compagnia telefonica non integrasse gli estremi di un'intercettazione, poiché rientrante nel complesso delle attività ordinariamente compiute dall'azienda e necessarie all'espletamento del proprio servizio. La giurisprudenza in proposito è giunta a sostenere che le conversazioni (e.g. *mail*) conservate su *server* dell'azienda, inclusi messaggi di posta elettronica inviati da o ricevuto in una casella di posta messa a disposizione del datore di lavoro, costituiscono proprietà di quest'ultimo. Vedi B.T. CROWTHER, (Un)Reasonable Expectation of Digital Privacy, 2012, *Brigham Young University Law Review*, 1, 2012, 343 ss.

[612] Si veda, in tal senso, *United States v. Maynard* (615 F.3d 544, 2010).

[613] Con più generico riguardo ad ipotesi di tracciamento degli spostamenti di indagati attraverso l'applicazione di dispositivi GPS sui veicoli si veda *United States v. Garcia* No. 18-1735 (7th Cir. 2019). Cfr. H. PLOURDE-COLE, Back to Katz: Reasonable Expectation of Privacy in the Facebook Age, 38, *Fordham Urb. L.J.*, 2, 2010, 571 ss; M.V. FORD, Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology, 19, *American University Journal of Gender Social Policy and Law*, 4, 2011, 1351ss; R. PRUNTY e A. SWARTZENDRUBER, *Social Media and the Fouth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 415-416.

[614] J.M. CASTELLANO, *Prosecutor's Manual for Arrest, Search and Seizure*, III ed., New York, LexisNexis, 2015, §18.02, spec. nt. 6.

polizia, perché si tradurrebbe in un ingiustificato vantaggio per i criminali[615]. Anche in questo caso, tuttavia, i tradizionali approdi giurisprudenziali hanno dovuto ricalibrarsi in ragione degli sviluppi tecnologici. In quest'ottica, non sorprende la posizione recentemente assunta dalla Corte Suprema nel caso *Carpenter v. United States* (No. 16-402, 585 U.S. 2018).

La decisione prese le mosse da un'indagine avviata su una rapina nel corso della quale uno degli arrestati, dopo aver confessato, consegnò il suo telefono all'FBI, la quale ottenne sì il via libera del giudice per l'accesso ai dati della geolocalizzazione del dispositivo, ma ai soli sensi dello *Stored Communications Act*[616]. Tale normativa, infatti, si limita a richiedere "*reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation*"[617]. Ottenuto così accesso allo storico della geolocalizzazione del dispositivo senza dover soddisfare il più stringere presupposto probatorio della *probable cause* di cui al Quarto emendamento, gli investigatori furono in grado di stabilire che il Sig. Carpenter si trovava nei pressi dei luoghi colpiti al momento delle rapine, sancendone la condanna in primo grado. La sentenza venne poi confermata in appello ove i giudici sottolinearono come, in linea con la *third-party doctrine* di *Smith v. Maryland*, "*cell-site data - like mailing addresses, phone numbers, and IP addresses - are information that facilitate personal communications, rather than part of the content of those communications themselves*[618]*."*

La Corte Suprema, tuttavia, investita della questione ritenne invece che la *third-party doctrine* non potesse essere applicata alla tecnologia in questione. Ciò in quanto, osservò la Corte, "*seismic shifts in digital technology* […] *made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike*

[615] Sempre in tema di utilizzo di dispositivi di geolocalizzazione, mostrando un atteggiamento più affine alla giurisprudenza pre-Katz, in *United States v. Pineda-Moreno* (591 F.3d 1212, 2010) la Corte ritenne che, nella misura in cui gli agenti non fossero materialmente entrati nel veicolo, l'utilizzo di strumentazione esterna non potesse costituire una perquisizione illegittima. Cfr. D. KLITOU, *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014, 213.

[616] Per una più puntuale disamina del contenuto di tale atto normativo si veda meglio *infra sub* §3.5.

[617] *Stored Communication Act*, Sec.2703(d).

[618] Cfr. S. KEFFER, Too Big to Surveil: The Fourth Amendment Illuminated By 'Modern Lights' and Shadowed By *Obsta Principiis* in a Post-Carpenter World Concerned With Privacy, 2, *Information & Communications Technology Law*, 28, 2019, 161 ss.

the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in Smith and Miller and the exhaustive chronicle of location information casually collected by wireless carriers today[619]*."* Per i Giudici, quindi, il caso presentava maggiori affinità con la pervasività tecnologica già ravvisata in *U.S. v. Jones* (565 U.S. 400, 2012), rendendo in tal modo necessario un previo mandato ai sensi del Quarto emendamento[620].

Da notare, però, come la sensibilità della Corte verso i nuovi scenari aperti dall'evoluzione tecnologica non abbia comunque indotto un completo abbandono dei retaggi dominicali sottesi all'esegesi del Quarto emendamento. Il Giudice Gorsuch, infatti, pur condividendo la conclusione della Corte, si discostò dalla motivazione addotta dalla maggioranza, ritenendo sufficiente osservare come l'interessato vantasse una posizione dominicale sui dati relativi alla propria geolocalizzazione, rendendo superflua l'invocazione di una "*reasonable expectation of privacy*[621]*"*.

Come già accennato, peraltro, un primo *revirement* in punto di utilizzazione di dispositivi GPS si era avuto già in *U.S. v. Jones* (565 U.S. 400, 2012). In tale caso, le forze dell'ordine avevano proceduto ad impiantare un dispositivo GPS sull'autoveicolo di Antoine Jones. Sebbene tale operazione fosse stata preceduta dall'accoglimento di una richiesta di mandato, il tracciamento degli spostamenti del sospettato avvenne al di fuori del limite temporale fissato dal giudice. Di conseguenza, discostandosi dal precedente orientamento per cui nessuna aspettativa di privacy poteva essere invocata sugli

[619] *Carpenter v. United States* (No. 16-402, 585 U.S. 2018), § B.

[620] Nelle parole del giudice Roberts: "[*t*]*he question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in Jones. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled*." *Carpenter v. United States* (No. 16-402, 585 U.S. 2018), § III.

[621] Nelle parole del Giudice "[*i*]*t seems to me entirely possible a person's cell-site data could qualify as his papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U. S. C. §222 designates a customer's cell-site location information as "customer proprietary network information" (CPNI), §222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves. The statute generally forbids a carrier to "use, disclose, or permit access to individually identifiable" CPNI without the customer's consent, except as needed to provide the customer's telecommunications services. §222(c)(1). It also requires the carrier to disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer." §222(c)(2). Congress even afforded customers a private cause of action for damages against carriers who violate the Act's terms. §207. Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right*." *Carpenter v. United States* (No. 16-402, 585 U.S. 2018), Justice Gorsuch, *dissenting opinion.*

spostamenti di un veicolo[622], la Corte ritenne integrati gli estremi della violazione della privacy, in virtù dell'elevato grado di invasività del tracciamento. In particolare, il Giudice Scalia, nella sua *concurring opinion*, tenne a sottolineare come nella "*pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case -constant monitoring of the location of a vehicle for four weeks- would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitorning relatively easy and cheap*[623]*.* "

L'esigenza di prendere in considerazione il carattere marcatamente ubiquitario delle nuove tecnologie, nonché il grado di dettaglio dalle stesse reso possibile nel ricostruire spostamenti, preferenze, abitudini e ogni altro aspetto della vita di una pletora di individui costantemente crescente, emerge ancora più chiaramente nelle parole del giudice Sonia Sotomayor. Quest'ultima, infatti, nella sua *concurring opinion* al caso Jones, sottolineò la necessità di riconsiderare "*the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks*[624]*.* "

Ciononostante, all'accresciuta sensibilità tecnologica delle Corti troppo spesso non corrisponde una maggiore prudenza degli utenti della rete[625]. Anzi, la diffusa assuefazione alle modalità digitali di esplicazione quotidiana delle dinamiche sociali fa troppo spesso sottovalutare la vulnerabilità che ne consegue. Fa riflettere, in tal senso, la decisione assunta nel caso *United States v. Meregildo* (883 F. Supp. 2d 523, 2012) in cui

[622] Così *United States v. Knotts* (460 U. S. 276, 281, 1983) per cui "[*a*] *person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another*."

[623] *U.S. v. Jones* (565 U.S. 400, 2012), §V. Cfr. D.J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011, 102ss.

[624] *U.S. v. Jones* (565 U.S. 400, 2012), Justice Sotomayor, concurring opinion. Cfr. B. KAMINS, *New York Search & Seizure*, New York, LexisNexis, 2019, 2063; J.A. ADAMS e D.D. BLINKA, *Prosecutor's Manual for Arrest, Search and Seizure*, II ed., New York, LexisNexis, 2270ss.

[625] Cfr. C.J. BORCHERT, F.M. PINGUELO, D. THAW, Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act, 13, *Duke L. & Tech. Rev*., 2013, 36, 41ss.

uno degli "amici" Facebook dell'indagato, accettò di cooperare con le forze dell'ordine mostrandogli quanto pubblicato dal primo sul suo profilo. In tal modo, gli agenti ottennero informazioni sufficienti a supportare la *probable cause* necessaria per l'emissione mandato che poi autorizzò l'accesso all'intero profilo Facebook. Lamentata la violazione del Quarto emendamento, la Corte ritenne che "*when a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected*." Nel caso di specie, quindi, avendo reso le informazioni condivise sul suo profilo accessibili ai suoi "amici", l'utente, pur potendo in astratto vantare la legittima aspettativa che le informazioni diffuse sulla piattaforma non fossero direttamente accessibili dalle forze dell'ordine, non poteva ragionevolmente estendere tale aspettativa ai terzi con cui tali dati sono stati spontaneamente condivisi [626].

Questa carrellata di precedenti giurisprudenziali, per quanto sintetica ed inevitabilmente parziale, rende comunque più che adeguatamente la misura di come l'assuefazione collettiva ai rischi introdotti dalle nuove abitudini digitali possa rendere irragionevole qualsivoglia aspettativa di privacy nel contesto digitale, svuotando di significato il Quarto emendamento, così come interpretato dalla giurisprudenza post Katz. Proprio in quest'ottica, parte della dottrina ritiene preferibile abbandonare il test della *reasonable expectation of privacy*, focalizzandosi invece su una aspettativa che guardi meno al regime di diffusione o condivisione delle informazioni, oggigiorno tendenzialmente scontato e in molti casi anzi auspicato, e si concentri maggiormente sulla ragionevolezza (*rectius* prevedibilità) delle finalità di utilizzo dei dati[627]. In particolare, l'esigenza di una siffatta evoluzione interpretativa sarebbe riconducibile all'emersione di

[626] In tal senso, la Corte affermò che "[*w*]*here Facebook privacy settings allow viewership of postings by 'friends', the Government may access them through a cooperative witness who is a 'friend' without violating the Fourth Amendment*." Cfr. R. PRUNTY e A. SWARTZENDRUBER, *Social Media and the Fouth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015, 417.

[627] M.E. LEONARD, *The Changing Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 324.

un progressivo divario tra le aspettative soggettive individuali e le oggettive modalità di circolazione delle informazioni in rete[628].

È noto, infatti, come la pervasività senza precedenti dei sistemi di monitoraggio introdotti dalla quarta rivoluzione industriale stiano progressivamente plasmando quella che Packard ha efficacemente definito una "*naked society*"[629]. In questo contesto è quindi indispensabile che il contrarsi fino scomparire di uno spazio materiale di imperscrutabilità dei pensieri[630], non si traduca in una contestuale contrazione dei diritti degli interessati. Al contrario, se è vero che la privacy è la condizione in cui "*we can exist in a way in which others do not know what we are doing*[631]*",* e se è vero che il raggiungimento di questo stato è sempre più spesso tecnologicamente impossibile[632], è compito del legislatore intervenire per rimuovere le barriere fattuali alla realizzazione di tale prerogativa.

Tutte le difficoltà e i dubbi ermeneutici fin qui sollevati rendono infatti evidente la crescente necessità di un chiaro quadro legislativo. Tale esigenza è bene espressa dalle parole del Giudice Scalia nella sua già menzionata *concurring opinion* in *United States v. Jones*, ove rimarca come "[*i*]*n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way*[633]*."*

---

[628] Secondo parte della dottrina, tale fenomeno è principalmente imputabile alle soluzioni contrattuali predisposte dagli ISP, all'ormai universale tendenza all'archiviazione online di risorse e informazioni, nonché all'impreparazione tecnologica dei protagonisti del mondo del diritto, a partire dai giudici. Cfr. B.T. CROWTHER, (Un)Reasonable Expectation of Digital Privacy, 2012, *Brigham Young University Law Review*, 1, 2012, 343 ss.

[629] V. PACKARD, *The Naked Society*, Brooklyn, Ig Publishing, 1964, 10.

[630] Emblematiche, in tal senso le parole di K. Leigh, per cui "*[i]t is possible that the only truly private communications we have are the thoughts in our heads*." Così ID., *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 2.

[631] M.E. LEONARD, *The Changing Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 309.

[632] Nelle parole utilizzate dalla Corte nel caso *Menard v. Mitchell* (328 F Supp 718, DC Cir, 1971): "*Systematic recordation and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom*. […] *If information available to Government is misused to publicize past incidents in the lives of its citizens the pressure for conformity will be irresistible. Initiative and individuality can be suffocated and a resulting dullness of mind and conduct will become the norm. […] In short, the overwhelming power of the Federal Government to expose [citizens' lives to public scrutiny] must be held in proper check*."

[633] Cfr. J.R. KANOVITZ, *Consitutional Law for Criminal Justice*, XIV ed., New York, Routledge, 2015, 657.

Da ricordare, peraltro, che tutti gli sviluppi giurisprudenziali sin qui analizzati e descritti con riguardo al Quarto emendamento, operano solo ed esclusivamente con riferimento ad azioni governative o di agenti governativi. È evidente, tuttavia, che l'impostazione socio-culturale sottesa alle giurisprudenza sviluppatasi intorno al Quarto emendamento non può che riflettersi anche sui rapporti interprivati[634].

Primo e paradigmatico esempio, infatti, ne è la disciplina federale dettata in materia di intercettazioni, i cui principi e limiti, oltre che rispecchiare e precisare gran parte delle conclusioni giurisprudenziali sin qui esaminate, sono una delle poche fonti federali suscettibili di dettare un argine legislativo al fenomeno dei processi decisionali automatizzati. Proprio in quest'ottica, quindi, l'analisi proseguirà, dapprima, con una ricostruzione dei settoriali frammenti legislativi che, complessivamente considerati, dettano la lacunosa disciplina federale in punto di comprensibilità dei processi decisionali automatizzati. In secondo luogo, ed a chiusura del capitolo, verranno rapidamente esaminati i più recenti tentativi compiuti dalla dottrina, in punto di *enforcement*, dal legislatore californiano, a livello statale, e dall'*American Law Institute*, a livello federale, di introduzione di una normativa onnicomprensiva in punto di *data privacy*, al fine di mettere in luce la direzione evolutiva assunta dall'ordinamento degli Stati Uniti in punto di protezione dei dati personali.

3.5. *Electronic Communication Privacy Act*: un divieto di intercettazioni unicamente automatizzate?

Lo *Electronic Communication Privacy Act* venne adottato nel 1986 al fine di modificare ed integrare la disciplina del *Federal Wiretap Act* del 1968 (oggi titolo I dello ECPA[635]) che, nel disciplinare le intercettazioni di conversazioni svolte a mezzo di linee telefoniche fisse, lasciava prive di tutela le più recenti forme di comunicazione elettronica e senza fili[636].

[634] M. ALLEN e A. ORHEIM, Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them, 8, *Wash. J. L. Tech. & Arts*, 2, 2012, 137 ss.

[635] Cfr. D.J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011, 73 ss.

[636] D.K. MULLIGAN, Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, 72, *Geo. Wash. L. Rev*., 2004, 1557, 1558.

Al fine di superare l'incertezza legislativa creata dall'innovazione tecnologica[637], la *House Committee on the Judiciary* e il *Senate Committee on Governmental Affairs* investirono l'*Office of Technology Assessment* (OTA) del compito di condurre uno studio sui rischi posti alle libertà civili dalla mancanza di regolamentazione in materia di accesso alle comunicazioni elettroniche. Il report dell'OTA, pubblicato nel 1985 con il titolo *Electronic Surveillance and Civil Liberties*, confermò i vuoti di tutela nelle comunicazioni tra computers e propose tre possibili soluzioni per colmarli: (i) estendere alle mail lo stesso livello di tutela della posta ordinaria (il cui accesso è subordinato al rilascio di un mandato); (ii) richiedere il previo mandato per l'accesso al contenuto della posta elettronica dal terminale del mittente e del destinatario rimettendo, invece, alle Corti la valutazione per i requisiti di accesso a tali dati per il tramite di ISP; ovvero (iii) rimettere la questione alle dinamiche di autoregolamentazione del mercato e al pragmatismo casistico delle Corti[638]. Con l'adozione dell'ECPA il legislatore statunitense concluse per una quarta via: fissare una serie di presupposti e garanzie procedurali per l'accesso al contenuto delle comunicazioni elettroniche tanto dai terminali del mittente e del destinatario, quanto dai server di terzi *providers*, seppure affievolendone la rigidità in tale secondo caso[639].

A seguito delle modifiche così apportate, l'ordinamento statunitense oggi limita l'accesso alle comunicazioni via cavo[640], così come alle conversazioni orali[641] ed

---

Cfr. S.L. SPLICHAL, The evolution of computer/privacy concerns: Access to government information held in the balance, 1, *Communication Law and Policy*, 2, 1996, 203ss.

[637] Nelle parole di Kastenmeier, una delle menti dello ECPA, "[*w*]*hen the Founders added the fourth amendment's protection against unreasonable searches and seizures to the Constitution, they did so to protect citizens' papers and effects. In those days an individual's private writing and records were kept within the home. That situation has changed drastically today. Many Americans are now using computer services, which store the bank records, credit card data, electronic mail and other personal data. If we fail to afford protection against governmental snooping in these files, our right of privacy will evaporate. Moreover, if we fail to protect the records of third-party providers, there will be a tremendous disincentive created against using these services*." 132 *Congressional Records* 14886 (1986).

[638] OFFICE OF TECH. ASSESSMENT, *Electronic Surveillance and Civil Liberties* (CONGRESSO DEGLI STATI UNITI, 1985).

[639] D.K. MULLIGAN, Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, cit., 1557, 1564-1565; M.L. RICH, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, 164, *U. Pa. L. Rev.*, 2016, 871ss.

[640] Tali comunicazioni sono definite come "*any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce*." SCA, §2510 (1)

[641] Intese come "*any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication*." SCA § 2510(2).

elettroniche[642]. In particolare, l'ECPA si articola in tre parti: il *Wiretap Act*[643], il *Pen Register Act*[644] e lo *Stored Communication Act*[645]. I primi due disciplinano la c.d. *prospective surveillance*, ovvero il monitoraggio delle conversazioni in corso. Più nello specifico, il *Wiretap Act* regola l'intercettazione del contenuto delle comunicazioni, mentre il *Pen Register Act* detta le regole per l'utilizzo di cc.dd. *noncontent information* come, ad esempio, i numeri telefonici digitati. Al contrario, lo SCA detta la disciplina della c.d. *retrospective surveillance*, ovvero il regime di accesso alle conversazioni archiviate[646].

Delle tre, il *Wiretap Act* è senz'altro la sezione che, ai fini dell'analisi qui condotta, merita maggiore attenzione. Parte della dottrina, infatti, si è interrogata sull'idoneità, oltre che l'opportunità, di sfruttare il divieto di intercettazioni intenzionali di conversazioni private per il tramite di dispositivi tecnologici ivi disciplinato per limitare il monitoraggio automatizzato del contenuto di comunicazioni elettroniche. Ciò in quanto, anche se inizialmente sviluppata per contrastare la diffusione di messaggi cc.dd. *spam*, l'analisi automatizzata del contenuto delle comunicazioni elettroniche ha visto rapidamente espandere i propri utilizzi ad ambiti quali la tutela di diritti di proprietà intellettuale, la lotta al terrorismo, la tutela della salute pubblica mentale (filtrando e segnalando linguaggi indicativi di tendenze suicide) e fisica (analizzando le ricerche *web* per, ad esempio, monitorare l'andamento di contesti epidemici)[647].

Prima di entrare nel merito del dibattito, tuttavia, è necessario effettuare una rapida ricognizione dei tratti salienti della disciplina dettata dall'ECPA iniziando proprio dal *Wiretap Act* che, introdotto in risposta all'espansione giurisprudenziale della tutela del

[642] Ai sensi del SCA §2510 (12) per comunicazioni elettroniche si intende "*any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce*". Da notare, tuttavia, che da tale nozione sono espressamente escluse le trasmissioni effettuate a mezzo di *tracking devices* (disciplinate in §3117 SCA).

[643] 18 U.S.C. §§2511-2522.

[644] 18 U.S.C. §§ 3121-3127.

[645] 18 U.S.C. §§ 2701-2711.

[646] D.K. MULLIGAN, Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, cit., 1557, 1566. Cfr. S.M. BELLOVIN, R.M. HUTCHINS, T. JEBARA, S. ZIMMECK, When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8, *N.Y.U. J. L. & Liberty*, 2014, 556ss.

[647] B.E. BOYDEN, Can a Computer Intercept your email?, 34, *Cardozo L. Rev.*, 2012, 669, 671. Cfr. J. GINSBERG , M.H. MOHEBBI, R.S. PATEL, L. BRAMMER, M.S. SMOLINSKI, L. BRILLIANT, Detecting influenza epidemics using search engine query data, 457, *Nature*, 2009, 1012; P. OHM, The Rise and Fall of Invasive ISP Surveillance, *U. Ill. L. Rev.*, 2009, 1417, 1427-32; A. KOZINSKI, The Dead Past, 64, *Stan. L. Rev. Online*, 2012, 117, 118-19.

Quarto emendamento all'intercettazione di conversazioni orali effettuate per il tramite di cabine telefoniche pubbliche inaugurata con il caso Katz, ne procedimentalizza il regime. In particolare, l'attore che lamenta l'illiceità di una c.d. "*aural acquisition*" deve dimostrarne il carattere intenzionale e l'impiego di strumenti elettronici, meccanici o altri dispositivi [648]. La controparte, dal canto suo, può difendersi provando che l'intercettazione è stata effettuata in modo accidentale, nel contesto dell'ordinario svolgimento delle proprie attività imprenditoriali (*business extension defense*)[649], ovvero previo consenso dell'interessato. Tale ultima eccezione può essere vinta dall'attore dimostrando il fine illecito dell'intercettazione a cui aveva originariamente acconsentito[650].

Lo *Stored Communication Act* (SCA), invece, come accennato, ha integrato la disciplina dell'ECPA al fine di colmare il vuoto di tutela creato dall'avvento delle comunicazioni elettroniche[651], protette purché non già pubbliche ovvero divulgate da un utente che vi ha avuto legittimo accesso[652]. Tale titolo, in particolare: (i) vieta l'accesso non autorizzato alle comunicazioni al fine di ottenere, alterare o distruggere conversazioni[653]; (ii) vieta, salvo alcune eccezioni, la divulgazione di tali conversazioni[654]; (iii) fissa garanzie procedurali per la richiesta governativa di accesso alle comunicazioni elettroniche per il tramite di ISP[655]. Peraltro, il grado di protezione

[648] Cfr. J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 312ss; B.E. BOYDEN, Can a Computer Intercept your email?, cit., 678. S.L. MARTIN, Interpreting the Wiretap Act: Applying Ordinary Rules of Transit to the Internet Context, 28, *Cardozo L. Rev*., 2006, 441ss.

[649] ECPA § 2511(2)(a)(i).

[650] Cfr. D.K. MULLIGAN, Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, cit., 1557, 1566.

[651] In quest'ottica, parte della dottrina ritiene che la scelta del legislatore statunitense di disciplinare le intercettazioni di comunicazioni elettroniche attraverso l'introduzione di un apposito titolo dell'ECPA implichi l'inapplicabilità, alle stesse, della disciplina del Wiretap Act. Per riflessioni sulle difficoltà affrontate dalla giurisprudenza nell'estendere analogicamente la disciplina del Wiretap Act alle comunicazioni elettroniche si veda S. FREIWALD, First Principles of Communications Privacy, Stan. Tech. L. Rev. 3, 2007, 36ss.

[652] Ad esempio, in *Ehling v. Monmouth-Ocean Hospital Service Corp*., sebbene la Corte avesse riconosciuto l'applicabilità dello SCA rispetto a "post" condivisi sulla piattaforma Facebook, la stessa rigettò la richiesta di risarcimento del danno avanzata dal lavoratore licenziato per informazioni, ivi condivise, a cui il datore di lavoro aveva avuto legittimo accesso attraverso un collega dell'attore, suo "amico" sul social network. In questo caso, sostennero i giudici, le informazioni erano state ottenute dal datore di lavoro in applicazione dell'eccezione del c.d. "*authorized access*" fissata dallo SCA. S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299, 317. Cfr. C. CRANE, Social Networking v. the Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking, 89, *Wash. U. L. Rev.*, 2012, 639, 642.

[653] 18 U.S.C. §2701.

[654] 18 U.S.C. §2702.

[655] Da notare, peraltro, che lo SCA distingue tra informazioni detenute da *electronic communication service providers*, da *remote computing service providers* ovvero da prestatori di servizi

riconosciuta alle comunicazioni elettroniche degrada progressivamente col passare del tempo: dalla *probable cause* richiesta per l'accesso a messaggi di posta elettronica non aperti e ricevuti da meno di 180 giorni, si passa alla mera rilevanza delle informazioni ai fini dell'indagine per l'intercettazione di comunicazioni archiviate elettronicamente da più di 180 giorni[656].

Infine, il *Pen Register Act* (titolo III dell'ECPA) disciplina l'utilizzo di dispositivi di registrazione di numeri digitati (cc.dd. *pen registers*) introducendo, all'indomani dell'orientamento assunto dalla Corte Suprema in *Smith v. Maryland*[657], un minimo di garanzie procedimentali per l'intercettazione di *transactional data* generati dal traffico telefonico. Ne consegue che la captazione dei numeri di telefono identificativi delle chiamate in entrata e in uscita è ammessa anche senza un vero e proprio mandato di cui al Quarto emendamento, ma comunque previa dimostrazione della rilevanza delle informazioni così ottenute ai fini di un'indagine in corso[658].

Ricostruita così sommariamente la portata normativa dell'ECPA e tornando a concentrare l'attenzione sul ruolo che il *Wiretap Act* è venuto, o meglio, non è venuto, ad assumere nel contesto digitale, un esempio paradigmatico dell'infruttuosità dei tentativi di calare il divieto di intercettazioni ivi disciplinato nel mercato *Data-Driven* è il caso *In re DoubleClick, Inc.*[659]. In tale occasione, infatti, la giurisprudenza statunitense ebbe modo di chiarire che il tracciamento dei dati di navigazione degli utenti attraverso l'utilizzo di *cookies* di profilazione della società di marketing personalizzato *DoubleClick* non integrasse gli estremi di una illegittima intercettazione delle interazioni online dei singoli con i siti web interessati. Ciò in quanto questi ultimi, parte degli scambi

che non rientrano in nessuna delle precedenti categorie come, ad esempio, nel caso di comunicazioni elettroniche gestite e archiviate dal datore di lavoro nel contesto di un'organizzazione aziendale che non si occupa di offrire servizi di comunicazione elettronica al pubblico, ma soltanto ai propri dipendenti. 18 U.S.C. §2703-2706, 2709. Cfr. D.J. SOLOVE, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011, 157ss; D.K. MULLIGAN, Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, cit., 1557, 1568.

[656] Cfr. B.E. BOYDEN, *Privacy of Electronic Communications*, in K.J. MATHEWS (a cura di), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, II ed., Practicing Law Institute, 2011, 6-30-40; J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J.*, 23, 2019, 23, 38.

[657] Sulla portata di tale pronuncia nel percorso giurisprudenziale di affermazione della data privacy negli Stati Uniti si veda quando osservato *supra sub para* §3.4.2.

[658] 18 U.S.C. § 3122 (b)(2). Cfr. J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J.*, 23, 2019, 23, 38.

[659] Cfr. D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, New York, 2004, 68ss.

informativi intercettati, avevano espressamente acconsentito all'attività di monitoraggio della prima[660].

Concentrando invece l'attenzione su quella specifica manifestazione del contesto *Big Data* che sono i processi decisionali automatizzati, come accennato in apertura del paragrafo, parte della dottrina si è interrogata circa l'applicabilità del *Wiretap Act* ad ipotesi in cui il monitoraggio (*rectius* l'intercettazione) del contenuto di comunicazioni elettroniche personali sia effettuato in modo esclusivamente automatizzato[661]. Secondo il prevalente orientamento, infatti, un trattamento esclusivamente automatizzato delle comunicazioni elettroniche non rientrerebbe nella nozione di intercettazione di cui al *Wiretap Act*[662] la quale, individuando nell'ascolto l'attività proibita, renderebbe di per sé irrilevanti sistemi meccanici di registrazione non strumentali a qualche forma di coinvolgimento umano[663].

Anche a seguito dell'ampliamento dell'ambito di applicazione della norma dal solo "*wiretapping"* a qualsiasi forma di "*electronic eavesdropping"* operato in sede di adozione dell'*Omnibus Crime Control and Safe Streets Act* del 1968, la giurisprudenza ha continuato ad interpretare il *Wiretap Act* nel senso di escluderne l'operatività in ipotesi prive di forme di coinvolgimento umano nell'accesso al contenuto delle conversazioni captate[664]. Ad esempio, in *United States v. Turk* i giudici fecero propria una nozione di "*aural acquisition*" implicante l'utilizzo del dispositivo tecnico di registrazione come un "*agent of the ear*" e, quindi, come un mero sostituto del primo ascolto da parte dell'agente

[660] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[661] S. FREIWALD, First Principles of Communications Privacy, 3, *Stan. Tech. L. Rev*., 2007, 1ss; C.R. GELLIS, CopySense and Sensibility. How the Wiretap Act Forbids Universities from Using P2P Monitoring Tools, 12, *B.U. J. Sci. & Tech. L*., 2006, 340.

[662] B.E. BOYDEN, Can a Computer Intercept your email?, cit., 669, 673. Critico anche R.A. POSNER, Privacy, Surveillance, and Law, 75 *U. Chi. L. Rev*., 2008, 245, 249; M. TOKSON, Automation and the Fourth Amendment, 96, *Iowa L. Rev*., 2011, 581.

[663] Nelle parole dell'Autore "*[s]uch automated processing does not by itself pose any threat to privacy. Although there is a tendency to anthropomorphize computers, just like we anthropomorphize cars and toasters, a computer scanning an email is the functional equivalent of a thermostat turning on the heat. A thermostat is not a surveillance device; it does not monitor a house and make a decision about what temperature the house should be. It mechanically triggers a switch according to its programming. Automated processing of communications is similar. There is therefore no need to erect a legal barrier to such processing to protect privacy, and the current Wiretap Act does not impose one*." B.E. BOYDEN, Can a Computer Intercept your email?, cit., 677-681 e 717. Cfr. G. R. BLAKEY e J.A. HANCOCK, A Proposed Electronic Surveillance Control Act, 43, *Notre Dame L. Rev*., 1968, 657, 661

[664] In *United States v. Rodriguez* 968 F.2d 130, 135-36 (2d Cir. 1992), ad esempio, i giudici ribadirono come la natura nella nozione di intercettazione fosse rimasta immutata a seguito delle modifiche apportate con l'adozione dell'ECPA, continuando a richiedere la ricezione umana o l'archiviazione a fini di successivo accesso da parte di un operatore umano. Cfr. BOYDEN, Can a Computer Intercept your email?, cit., 689.

umano. In caso contrario, osservò la Corte, ogni riproduzione di conversazioni precedentemente registrate costituirebbe una nuova violazione del *Wiretap Act*[665].

D'altro canto, come messo in evidenza nel caso *People v. Bialostok*, seppure la disciplina delle intercettazioni, a differenza della *third-party doctrine*, prescinda dalle aspettative degli interessati e dal concreto regime di utilizzo dei loro dati, dare esclusivo rilievo alla dimensione di astratta ed ipotetica invasività delle tecnologie impiegate, finirebbe per rendere virtualmente illegittimo qualsiasi utilizzo dei dati da parte di ISP. Questi ultimi, infatti, nel contesto *data-driven*, sono sempre più spesso indotti a dotarsi di infrastrutture tecnologiche potenzialmente idonee ad effettuare trattamenti ben più ampi di quelli comunicati agli utenti e/o necessari allo svolgimento delle ordinarie attività del titolare[666].

Tale consapevolezza, tuttavia, non dovrebbe tradursi in una attitudine interpretativa cauta al punto da trascurare completamente le importanti tutele che, in un contesto normativo lacunoso come quello statunitense, il *Wiretap Act* può offrire rispetto a prassi aziendali particolarmente invasive, come quelle basate sulla scansione automatizzata del contenuto di comunicazioni elettroniche private a fini di marketing personalizzato[667].

La questione emerse per la prima volta con il lancio del servizio gratuito di posta elettronica di Google, finanziato, al pari del motore di ricerca, attraverso i proventi di un *behavioral advertising* asseritamente alimentato dal contenuto delle comunicazioni scambiate su Gmail. Gran parte della clientela, tuttavia, mostrò forti riserve rispetto a

---

[665] *United States v. Turk* 526 F.2d 654 (5th Cir. 1976), 658. Tale posizione è stata sostanzialmente condivisa dalle altre Corti che, in più occasioni, hanno avuto modo di chiarire come sia l'atto di utilizzare il dispositivo di registrazione (o, più genericamente, intercettazione) al fine di consentire il successivo accesso alla conversazione a rilevare ai sensi della disciplina in esame, a prescindere dall'effettivo ascolto della stessa. In questo senso, *ex multis*, *United States v. Lewis*, 406 F.3d 11, 18 n.5 (1st Cir. 2005). In *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994), invece, la Corte ritenne che le mere registrazioni fossero venute ad avere rilevanza ai sensi del *Wiretap Act* solo a seguito delle modifiche apportate con l'ECPA, per effetto del quale la disciplina è stata estesa alle "altre forme di acquisizione" e non solo a quelle operate per via dell'ascolto. Al contrario, invece, un orientamento minoritario ha escluso la rilevanza, ai sensi del *Wiretap Act*, di registrazioni non ascoltate. In questo senso, ad esempio, *Greenfield v. Kootenai Cnty*., 752 F.2d 1387, 1389 (9th Cir. 1985); *By-Prod Corp. v. Armen-Berry Co*., 668 F.2d 956, 960 (7th Cir. 1982).

[666] E. BOYDEN, Can a Computer Intercept your email?, cit., 697-698. Cfr. D.J. SOLOVE, *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, New York, 2004, 204 ss.

[667] M.R. CALO, The Boundaries of Privacy Harm, 86 *Ind. L.J.*, 2011, 1131, 1146-52; P. OHM, The Rise and Fall of Invasive ISP Surveillance, *U. Ill. L. Rev.*, 2009, 1417, 1444ss. Cfr. A. KOZINSKI, The Dead Past, 64, *Stan. L. Rev. Online*, 2012, 117, 118-19.

quella che venne percepita come un'indebita ingerenza nelle proprie conversazioni private. Riserve che, soltanto in parte placate dall'annuncio delle modalità unicamente automatizzate del processo di scansione[668], sfociarono in un'azione di classe avviata da utenti non Gmail nei confronti di Google, accusata di aver sfruttato il programma di scansione automatizzata per monitorare il contenuto dei propri messaggi di posta elettronica a fini pubblicitari. In particolare, gli attori sostennero che, monitorando il contenuto di *emails* inviate da mittenti privi di un *account* Gmail e ricevute da utenti di tale servizio, Google avesse violato, fra gli altri, il divieto di intercettazioni di cui al *Wiretap Act*[669].

L'accordo transattivo raggiunto nel luglio 2017 con cui Google si è impegnato a interrompere (per un periodo di tre anni) qualsivoglia scansione automatizzata a fini pubblicitari della posta elettronica inviata a indirizzi Gmail, ha impedito una pronuncia nel merito. Rimane, quindi, dubbia la possibilità di applicare la disciplina dell'ECPA ad attività di profilazione a mezzo scansione automatizzata del contenuto di comunicazioni elettroniche. Se è vero, infatti, che la definizione di "contenuto" fatta propria dal *Wiretap Act* sia sufficientemente ampia da ricomprendere la sostanza, il senso o il significato di un messaggio, è altrettanto vero che, in mancanza di un generale divieto di trattamento di dati personali e/o di processi decisionali automatizzati, le menzionate categorizzazioni statunitensi del concetto di privacy presuppongono l'accesso, lo scambio o comunque la disseminazione di informazioni fino a quel momento ritenute riservate[670].

---

[668] J.I. MILLER, Don't Be Evil: Gmail's Relevant Text Advertisements Violate Google's Own Motto and Your E-Mail Privacy Rights, 33, *Hofstra L. Rev*, 2005, 1607; R.A. POSNER, Privacy, Surveillance, and Law, 75 *U. Chi. L. Rev*., 2008, 245, 249.

[669] Caso *Matera v. Google Inc*., 5:15-cv-04062 LHK.Cfr. C. BOWMAN, J. GRANT, *A Marketplace for Privacy: Incentives for Privacy Engineering and Innovation*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018, 451ss.

[670] Richiamando la categorizzazione di Daniel Solove sono distinte sei teorie di privacy come: (i) diritto ad essere lasciati soli; (ii) controllo sull'accesso al sé (definito da Ruth Gavison come "*the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention*"); (iii) diritto a non veder divulgate al pubblico informazioni tenute segrete sulla propria persona; (iv) diritto ad avere il controllo sulla conoscenza che gli altri hanno della propria persona (così Charles Fried); (v) il diritto di decidere quando, come e in che misura condividere informazioni personali con altri (così Alan Westin); (vi) complesso di pratiche sociali suscettibili di incidere e modificare i comportamenti degli interessati (come, nella esemplificazione di Solove, nel caso della divulgazione di segreti e della sorveglianza). Cfr. D.J. SOLOVE, Conceptualizing Privacy, 90, *Calif. L. Rev.*, 2002, 1087, 1088-90; S. SIMITIS, Reviewing Privacy in an Information Society, 135, *U. Pa. L. Rev*., 1987, 707, 708; H. NISSENBAUM, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, 2010, 186 ss; R. GAVISON, Privacy and the Limits of Law, 89, *Yale L.J.*, 1980, 421, 438; R.A. POSNER, The Economics of Justice, Harvard University Press, Cambridge (MA),

Ne conseguirebbe che, come sostenuto da Ohm, il carattere meramente automatizzato del trattamento sarebbe garanzia di neutralità e, anzi, strumento di prevenzione di quei coinvolgimenti umani indesiderati che il *Wiretap Act* mira a sanzionare[671]. In senso contrario, Chopra e White sottolineano l'irrilevanza della natura automatizzata dei mezzi di trasmissione di informazioni personali ove, anche in assenza di coinvolgimento umano, la macchina sia in grado di produrre una conoscenza tale da incidere sui processi di formazione dei comportamenti, dello stato mentale e, in ultima analisi, dell'autonomia degli interessati[672], intesa come "*a zone of relative insulation from outside scrutiny and interference-- a field of operation within which to engage in the conscious construction of self*[673]*."*

A fronte di tale irrisolta incertezza interpretativa, ed in attesa di ulteriori chiarimenti legislativi o giurisprudenziali, non resta che auspicare l'adozione di un approccio interpretativo flessibile e sensibile a quella accezione di riservatezza che Helen Nissenbaum ha definito *contextual privacy*, identificandola nel complesso di aspettative sociali sulle modalità di circolazione delle informazioni. L'assunzione di una prospettiva estrinseca e relativa allo specifico contesto storico-culturale di riferimento, infatti, consentirebbe di individuare nelle reazioni degli interessati l'indice di una violazione dei principi di *data privacy* vigenti in un dato contesto[674]. In altri termini, Nissenbaum ravvisa una violazione della *contextual privacy* ogni qualvolta il trattamento dei dati determini un cambiamento dei destinatari, degli interessati o dei soggetti talmente inaspettato da generare diffidenza e timore negli interessati[675].

1981, 271; A. WESTIN, *Privacy and Freedom*, II ed., New York, Ig Publishing, 2015; C. FRIED, Privacy, 77, *Yale L.J.*, 1968, 475, 483.

[671] P. OHM, The Rise and Fall of Invasive ISP Surveillance, *U. Ill. L. Rev.*, 2009, 1417, 1427-32. In senso analogo si è espresso anche D.J. SOLOVE, A Taxonomy of Privacy, 154, *U. Pa. L. Rev*., 2006, 477, 495. Cfr. E. BOYDEN, Can a Computer Intercept your email?, cit., 707.

[672] S. CHOPRA, L.F. WHITE, *A Legal Theory for Autonomous Artificial Agents*, University of Michigan Press, Ann Arbor, 2011, 108 ss.

[673] J.E. COHEN, Examined Lives: Informational Privacy and the Subject as Object, 52, *Stan. L. Rev*., 2000, 1373, 1424.

[674]H. NISSENBAUM, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, 2010, 180ss.

[675] E. BOYDEN, Can a Computer Intercept your email?, cit., 708.

3.6. La "spiegazione" delle decisioni prese nel contesto della *Credit Reporting Industry*

Uno dei settori in cui l'utilizzo dei processi decisionali automatizzati è proliferato è quello dei sistemi di credito ai consumatori, fondati sull'accesso a *consumer files* e *credit scores*, sempre più frequentemente predisposti attraverso processi algoritmici, spesso oggetto di diritti di proprietà intellettuale[676].

L'azienda leader del settore è senza dubbio FICO, il cui modello di *credit scoring* è il più utilizzato negli Stati Uniti e, come correttamente osservato, il *credit score* è la più importante fra le informazioni che tradizionalmente confluiscono nei *consumer report* creati dalle agenzie di *Credit Reporting* (CRAs)[677]. Per quanto prevalente, tuttavia, quello di FICO non è l'unico modello algoritmico di calcolo di punteggi di credito. Ne consegue che gli individui vengono spesso a vedersi assegnati tanti diversi *credit scores* quanti sono gli algoritmi sviluppati delle diverse CRAs[678].

Inoltre, se, tradizionalmente, la quantificazione del merito creditizio si fondava su informazioni di natura finanziaria quali la puntualità nei pagamenti, il numero, la tipologia e l'ammontare dei finanziamenti e degli altri debiti in capo al cliente, le nuove richieste di credito, *etc*., l'ingresso nell'era dei *Big Data* ha determinato un progressivo ampliamento della pletora di informazioni utilizzate dalle CRAs (in parte acquistate presso *Data Brokers* ed in parte autonomamente acquisite attraverso il tracciamento dei dati di navigazione online e degli altri *user-generated contents*[679]*)*.

L'utilizzo dei *Big Data*, infatti, integrando la base informativa dei modelli tradizionali, non soltanto ne migliora la precisione, ma rende possibile la quantificazione del merito creditizio di soggetti che, non possedendo un patrimonio informativo

[676] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 50.

[677] *Fair Credit Reporting* (The consumer credit and sales legal practice series, NATIONAL CONSUMER LAW CENTER, IX ed.), 2017, § 16.1.

[678] *Big Data: A Tool For Inclusion Or Exclusion? Understanding the Issues* (FEDERAL TRADE COMMISSION, 2016).

[679] V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1710.

tradizionale sufficiente, sarebbero generalmente esclusi dal circuito creditizio (i cc.dd. *credit invisibles* o *unscoreables*[680]*).*

Dal canto loro, le società di c.d. *alternative lending*, avvalendosi di un approccio "*all data is credit data*[681]*"*, possono valutare il merito creditizio della clientela in pochi minuti e senza la necessità di un *credit score*[682], sfruttando i sistemi di *Machine Learning* per inferire la capacità di potenziali clienti di ripagare puntualmente eventuali finanziamenti[683]. L'accresciuta complessità tecnologica dei modelli alternativi di calcolo di punteggi di credito, noti come *e-scores* o *altscores*[684], tuttavia, aggrava l'opacità di processi decisionali che, per definizione, e prendendo in prestito le parole di Frank Pasquale, "*cannot be fully understood, challenged, or audited either by the individuals scored or by the regulators charged with protecting them*[685]*".* Inoltre, e al di là della più volte sottolineata tendenza di tali valutazioni automatizzate ad emulare *pattern* discriminatori insiti nel contesto sociale da cui i dati sono estrapolati [686], le società che sviluppano *altscores*, non qualificandosi sempre come CRAs, vengono potenzialmente a collocarsi al di fuori dell'ambito di applicazione della disciplina dettata per queste ultime[687].

Il sistema di *credit scoring* sin qui descritto pone quindi tre principali problematiche: (i) il rischio di precludere l'accesso al credito a candidati meritevoli a causa dell'implementazione di processi di valutazione del merito creditizio inaffidabili; (ii) le difficoltà di rilevare eventuali errori a causa dell'adozione di procedure di rettifica

[680] Secondo il Report del Consumer Financial Protection Bureau, al 2010 circa l'11% dei consumatori statunitensi risultava "*credit invisible*" mentre un altro 8,3% veniva ritenuto "*unscorable*". K.P. BREVOORT, P. GRIMM, M. KAMBARA, *Data Point: Credit Invisibles* (CONSUMER FIN. PROT. BUREAU OFFICE OF RESEARCH, 4), 2015. Cfr. V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1717.

[681] J. ADEBAYO, M. HURLEY, Credit Scoring in the Era of *Big Data*, 18, *Yale J.L. & Tech*., 2016, 148, 185-87.

[682] Cfr. C. O'NEIL, *Weapons of Math Destruction*, Broadway Book, New York, 2016, 147 ss.

[683] S. LOHR, Banking Start-Ups Adopt New Tools for Lending (*N.Y. Times*, 18 gennaio 2015); L. GENSLER, What's in a Score? Why More Lenders Are Using Alternative Data to Approve You for a Loan (*Forbes*, 8 agosto 2017).

[684] M. SEGAL, *What Is Alternative Finance?* (OFFICE OF ADVOCACY, U.S. SMALL BUSINESS ADMINISTRATION), 2016; S. BAROCAS, A.D. SELBST, *Big Data*'s Disparate Impact, 104, *Calif. L. Rev*., 2016, 671.

[685] F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015, 25.

[686] S. BAROCAS, A.D. SELBST, *Big Data*'s Disparate Impact, 104, *Calif. L. Rev*., 2016, 671, 678ss.

[687] V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1711.

complesse e inefficaci[688]; e (iii) l'esclusione finanziaria di importanti fasce della popolazione prive di una adeguata storia finanziaria e perciò irrimediabilmente impossibilitata ad ottenere un punteggio di credito[689].

In tale contesto, il legislatore statunitense è intervenuto con due principali leggi federali: il *Fair Credi Reporting Act* (FCRA) e l'*Equal Credit Opportunity Act* (ECOA). Entrambe, rivestono primaria rilevanza ai fini dell'analisi condotta nel presente capitolo in quanto, da un lato, recano specifici diritti informativi che, pur prescindendo dal carattere automatizzato o "manuale" del processo decisionale, si declinano in termini affini (seppure non sempre equivalenti) a quelli fissati dagli articoli 13-15 e 22 GDPR; e, dall'altro, operano nei confronti di enti statunitensi (prime fra tutte le agenzie di *credit reporting* Experian e FICO) che trattano anche dati provenienti dall'Unione europea e che, prima della sua recente invalidazione, avevano autocertificato l'adesione al *Privacy Shield*[690].

È perciò all'analisi della disciplina dettata dal FCRA e dall'ECOA che verrà, rispettivamente, dedicato il proseguo del paragrafo.

3.6.1. La consumer disclosure del Financial Credit Reporting Act

Il progetto legislativo poi sfociato nel FCRA fu inizialmente promosso dal Senatore Proxmire con il principale obiettivo di assicurare maggiore precisione e riservatezza delle informazioni raccolte dalle *credit bureaus*, le cui prassi aziendali troppo

[688] Uno dei principali problemi generalmente sollevati dagli interessati è quello della erroneità delle informazioni incluse nei fascicoli personali degli utenti, con conseguenti ripercussioni sul loro punteggio di credito. È questo, ad esempio, il caso di Patricia Armour che, avendo notificato all'agenzia Experian l'inesattezza delle informazioni raccolte sulla propria condizione finanziaria, dovette attendere oltre due anni e coinvolgere il *General Attorney* per ottenere una rettifica. Problematiche analoghe sono state sollevate anche nel caso, apparentemente opposto, in cui le inesattezze sulla condizione lavorativa dell'interessato ne davano una rappresentazione scorretta ma in *melius* (caso *Robins v. Spokeo* sul quale si dirà meglio *infra sub* § 3.6.).

[689] V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1713. Cfr. *Analysis of Difference Between Consumer and Creditor purchased Credit Scores* (CONSUMER FIN. PROT. BUREAU, 2012.

[690] La lista degli enti che avevano autocertificato la propria adesione al Privacy Shield è attualmente disponibile su un apposito sito web curato dal *Department of Commerce* degli Stati Uniti accessibile all'indirizzo *www.privacyshield.gov/list*.

spesso si traducevano in valutazioni del merito creditizio della clientela fondate su dati erronei, incompleti o di dubbia rilevanza. In quest'ottica, l'intervento normativo mirava a contrastare il fenomeno attraverso l'introduzione di standard pubblici di riservatezza e corretto utilizzo delle informazioni raccolte dagli operatori del settore del *credit scoring*[691].

La precoce rilevanza assunta dalla circolazione dei dati nella *consumer credit reporting industry* è peraltro confermata dalla circostanza per cui il FCRA, adottato nel 1970, è la prima legge statunitense in materia di *data privacy*.

La normativa si applica alle *consumer reporting agencies* definite come *"any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports*[692]*."* Inoltre, per effetto delle modifiche apportate dal *Consumer Credit Reporting Reform Act* del 1996, il medesimo regime normativo è stato esteso anche ai soggetti che utilizzano i *consumer reports*[693] emessi dalle prime come, ad esempio, banche e società finanziarie[694], nonché a coloro

[691] In questo senso, nel definire l'obiettivo perseguito dal Congresso con l'adozione del FCRA, la disposizione di apertura alla disciplina sul *credit reporting* chiarisce espressamente come "(1) [*t*]*he banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system.* (2) *An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.* (3) *Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers*. (4) *There is a need to ensure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy*." Così 15 USCA § 1681 (a). Cfr. 115 CONGRESSIONAL RECORDS 2410, 2411 (1969). Più in generale, per una ricognizione del quadro normativo statunitense nel settore del Fintech, con specifico riguardo all'adozione di strumenti computazionali automatizzati per finalità di erogazione del credito, si veda K. JOHNSON, F. PASQUALE, J. CHAPMAN, Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation, 88, *Fordham L. Rev*., 2019, 499ss.

[692] Così 15 USCA § 1681a(f). Ne sono esempi Experian, Transunion e Equifax. V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1723.

[693] In questo contesto, per *consumer reports* si intendono le comunicazioni rilasciate da *consumer reporting agencies* (CRA) con riguardo alla valutazione del merito creditizio, alla capacità e storia finanziaria, nonché alla personalità e più genericamente alla reputazione di clienti, utilizzati per assumere determinazioni rientranti nell'ambito di applicazione materiale del FCRA. Così 15 USCA § 1681a (d)(1). Cfr. S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299, 304.

[694] Sulla nozione di *users* si veda anche la definizione formulata in *Fair Credit Reporting* (The consumer credit and sales legal practice series, NATIONAL CONSUMER LAW CENTER, IX ed.), 2017, § 7.1.4.2.

che forniscono informazioni utili a fini di *consumer-reporting*, come i gestori di strumenti di pagamento [695].

Quanto ai settori industriali interessati dal FCRA, sebbene quest'ultimo presenti un campo d'applicazione indubbiamente più ristretto del GDPR, si presenta comunque come la normativa federale in materia di *data privacy* a maggior portata trans-settoriale. Nel disciplinare le finalità legittimamente perseguibili attraverso processi di *consumer reporting*, infatti, il FCRA non indica soltanto la concessione di finanziamenti o altre agevolazioni finanziarie, ma anche la sottoscrizione di polizze assicurative, lo svolgimento di procedure di assunzione o di altri processi valutativi in ambito lavorativo, nonché la concessione di licenze o altri sussidi pubblici[696]. Più ristretto, invece, il regime di utilizzo dei *consumer reports* a fini di marketing dei prodotti finanziari, ammesso soltanto ove comunicato al consumatore, ovvero ove a quest'ultimo siano offerti strumenti semplici per manifestare la volontà di opporsi a tale pratica[697].

In quest'ottica nella nozione di CRAs vengono ad essere ricomprese non soltanto le tradizionali agenzie di *credit scoring* attive su base nazionale (come Equifax, TransUnion e Experian), ma qualsiasi altro ente deputato alla creazione di fascicoli personali di consumatori allo scopo di valutarne tratti comportamentali e di personalità (cc.dd. "*specialty CRAs*") come, ad esempio, "*tenant screening bureaus*", "*check approval services*", e "*employment screening agencies*"[698].

Venendo al contenuto dei diritti e dei doveri ivi disciplinati, il FCRA fissa un modello di protezione tripartito, consistente in: (i) doveri informativi di notifica; (ii) procedure amministrative di risoluzione delle controversie; e (iii) rafforzamento dello standard probatorio per l'accesso governativo a tali informazioni[699]. Concentrando l'attenzione sul primo pilastro, di maggiore interesse ai fini dell'analisi qui condotta, il FCRA riconosce specifici diritti individuali in capo ai soggetti interessati, quali il diritto di essere informati ove un *credit report* venga utilizzato per prendere determinazioni nei

[695] 15 USCA § 1681a (r), (s) e (t).
[696] 15 USCA § 1681b.
[697] 15 USCA § 1681s-3.
[698] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 54.
[699] Posizione critica rispetto all'effettività dei rimedi messi a disposizione dal FCRA è stata espressa dalla corte distrettuale del Minnesota in *Henry v. Forbes* (433 F Supp 5, 1976).

propri confronti, il diritto di accederne al contenuto[700] e contestarne l'eventuale incompletezza o erroneità, nonché il diritto di conoscere il proprio *credit score*[701].

Infine, con il *Fair and Accurate Credit Transactions Act* del 2003 la disciplina del FCRA è stata integrata con misure precipuamente finalizzate a contrastare frodi e furti d'identità[702]. Più specificatamente, è stata prevista la configurabilità di un c.d. *security freeze* attraverso il quale inibire la trasmissione del proprio fascicolo da parte delle agenzie di *credit reporting* ovvero, in alternativa, la facoltà di attivare un *fraud alert* attraverso il quale evitare che informazioni riconducibili ad utilizzi fraudolenti dei propri dati confluiscano nel proprio *consumer report* ovvero incidano sul proprio *credit score*[703].

Fra tutti i diritti informativi disciplinati dal FCRA, nell'analisi dell'adeguatezza delle misure di salvaguardia predisposte dall'ordinamento statunitense avverso processi decisionali automatizzati suscettibili di incidere significativamente sulla sfera giuridica degli interessati, particolare attenzione merita il regime di *consumer disclosure* di cui alla sezione 1681g del Titolo XV dello *United States Code*.

Come accennato, in virtù di tale disposizione, ogni CRA è tenuta ad informare gli interessati del loro diritto di ottenere una copia del proprio *credit report*, di contestare le informazioni ivi contenute, nonché di ottenere un *credit score*[704]. Inoltre, ove l'interessato eserciti tale diritto facendone espressa richiesta, la CRA è altresì tenuta ad indicare le fonti da cui ha ottenuto le informazioni incluse del *credit report*, nonché l'identità di tutti i soggetti a cui, nell'arco dei dodici mesi precedenti la richiesta, è stato trasmesso[705]. Inoltre, ove l'interessato faccia richiesta di accesso al proprio c*redit score*, l'agenzia, seppure dietro pagamento di una "*fair and reasonable fee*"[706], è tenuta a fornire al consumatore informazioni concernenti: (i) la circostanza per cui il proprio modello di *credit scoring* potrebbe essere diverso da quello utilizzato dal finanziatore; (ii) il *credit*

[700] Quanto al regime di accesso ai credit reports, la sezione 1681 (a)(4) del FCRA disciplina il diritto degli interessati di conoscere la natura, la fonte e il contenuto dei propri dati personali raccolti dalle CRAs.

[701] Per la disciplina dei diritti di accesso al fascicolo da parte dei consumatori si veda 15 U.S.C.A. § 1681g.

[702] *Forty Years of Experience with the Fair Credit Reporting Act* (FEDERAL TRADE COMMISSION, luglio 2011), 3.

[703] Sul blocco del flusso informativo relativo ad attività compiute a seguito di furto d'identità si veda 15 U.S.C.A. § 1681c-2. Cfr. J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J.*, 23, 2019, 23, 35.

[704] 15 U.S.C.A. § 1681g (a) (B).

[705] 15 U.S.C.A. § 1681g (a).

[706] 15 U.S.C.A. § 1681g (f) (8).

scoring attualmente assegnato al richiedente nonché quello precedente più recente calcolato dall'agenzia per scopi collegati all'estensione di un finanziamento; (iii) l'intervallo dei valori minimi e massimi in cui oscilla il modello di *credit scoring*; (iv) i fattori principali (di regola non superiori a quattro) che hanno inciso negativamente sul proprio punteggio, (v) la data di elaborazione del *credit score*, nonché (vi) le fonti delle informazioni utilizzate per il calcolo dello stesso[707].

Tale previsione merita alcune ulteriori precisazioni, fondamentali alla piena comprensione della portata dei diritti informativi disciplinati dal FCRA.

Innanzitutto, tale regime di *disclosure* è limitato a richieste aventi ad oggetto una specifica tipologia di *credit scores*, ovvero quelli sviluppati per compiere previsioni circa il *credit behavior* dei clienti ed utilizzati per erogare prestiti. La fattispecie è, peraltro, ulteriormente ristretta dal legislatore per effetto dell'espressa esclusione di cc.dd. *mortgage scores* sviluppati nell'ambito di sistemi automatizzati di sottoscrizione di mutui che prendono in considerazione fattori ulteriori rispetto alle informazioni creditizie[708]. Ne consegue che rispetto a tutte le altre tipologie di cc.dd. *specialty scores* calcolati, ad esempio, in ambito assicurativo o lavorativo, agli interessati non è attribuito alcuno dei diritti informativi summenzionati[709].

In secondo luogo, la portata esplicativa del quadro informativo ivi disciplinato è fortemente attenuata in quanto, sebbene il FCRA imponga alle CRAs di formare del personale precipuamente deputato a spiegare le informazioni fornite ai consumatori in ottemperanza dei doveri di *disclosure* in esame[710], tali spiegazioni si traducono in una generica descrizione del modello di *credit scoring* che, per quanto utile, non consente al consumatore di conoscere lo specifico punteggio utilizzato dal finanziatore o l'incidenza che lo stesso ha prodotto sulla sua decisione di concedere o meno il credito, ma soltanto di meglio orientare *pro futuro* la propria condotta al fine di ottenere un miglior punteggio[711].

---

[707] 15 U.S.C.A. § 1681g (f) (1).

[708] 15 U.S.C.A. § 1681g (f) (2) (A).

[709] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 65.

[710] 15 U.S.C.A. § 1681h (c).

[711] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S.*

Per questo motivo i *credit scores* per tal via divulgati e "spiegati" sono anche definiti *educational scores*. La finalità educativa è tradizionalmente ricondotta alla disciplina sulle *adverse action notices* che, perciò, in tale prospettiva teleologica viene ad avvicinarsi alla *ratio* sottesa alle già menzionate teorizzazioni dottrinali sulle cc.dd. spiegazioni controfattuali. Ne consegue che, al pari di queste ultime, e per tutte le medesime ragioni in precedenza argomentate[712], il regime esplicativo fissato dal FCRA non è idoneo ad integrare gli estremi di una informazione significativa sulla logica utilizzata nei processi decisionali automatizzati di cui agli articoli 13-15 e 22 GDPR.

Diritti di spiegazione in parte più affini al regime fissato dal GDPR sono invece rinvenibili con riguardo a determinazioni in materia di mutui, *adverse action* e mercato del lavoro.

Rispetto al primo profilo, il FCRA dispone che, ove si avvalga di *credit scores* per valutare la richiesta di mutui o aperture di credito garantite da ipoteche su immobili ad uso abitativo (cc.dd. *home loan applications*), il finanziatore, oltre a dover fornire all'interessato tutte le generiche informazioni di cui alla descritta sezione (f), è anche obbligato a comunicare lo specifico *credit scoring* utilizzato[713]. Anche in questo caso, però, la portata esplicativa delle informazioni fornite, per quanto meno generica, è comunque difficilmente equiparabile a quella di cui agli articoli 13-15 e 22 GDPR. Come chiarito dal legislatore, infatti, tale regime di *disclosure* non coinvolge informazioni diverse dal *credit score* e dai cc.dd. *key factors*[714] che lo hanno influenzato, né impone un dovere di spiegazione di tali informazioni[715]. Peraltro, ove il punteggio non sia stato ottenuto da una CRA perché, ad esempio, elaborato con modelli sviluppati dallo stesso finanziatore, quest'ultimo potrà omettere la divulgazione dello specifico *credit score* utilizzato offrendo, ancora una volta, un mero *educational score* richiesto per l'occasione

Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law (COMMISSIONE EUROPEA, 2018), 65.

[712] Sull'impossibilità per le spiegazioni controfattuali di soddisfare la soglia di significatività fissata dal GDPR si veda meglio quanto osservato *supra sub* § 2.4.

[713] 15 U.S.C.A. § 1681g (g)(1).

[714] Ai sensi del FCRA per "*key factor*" si intendono "*all relevant elements or reasons adversely affecting the credit score for the particular individual, listed in the order of their importance based on their effect on the credit score*". 15 U.S.C.A. § 1681g (f)(2)(B).

[715] 15 U.S.C.A. § 1681g (g) (1)(E).

ad una CRA[716]. Stessa esenzione vale, inoltre, per il caso in cui il finanziatore si avvalga di sistemi automatizzati di sottoscrizione dei prestiti[717].

Parzialmente più esplicativi, risultano i doveri informativi che il FCRA disciplina per il caso di *adverse action notices*[718]. In particolare, ogniqualvolta un soggetto assuma determinazioni sfavorevoli al cliente in specifici settori (quali, ad esempio, quello assicurativo, finanziario o lavorativo), quest'ultimo ha diritto ad ottenere una notifica orale, scritta o elettronica recante l'indicazione della misura adottata, dello specifico *credit score* su cui si è fondata in tutto in parte la decisione, del nominativo dell'agenzia che ha fornito il *credit report*, nonché della circostanza per cui quest'ultima non è stata direttamente coinvolta nella decisione relativa all'*adverse action* e, perciò, non può fornire alcun chiarimento sui motivi della stessa[719].

Questi ultimi, quindi, rimangono ancora una volta esclusi dalla portata dei doveri informativi disciplinati dal FCRA. Anche nel caso in cui il consumatore sfrutti il termine di sessanta giorni che la normativa mette a sua disposizione per richiedere le ragioni alla base dell'*adverse action* adottata sulla base di informazioni ottenute da terze parti diverse da CRAs, il decisore non sarà tenuto a divulgare la logica che ha condotto alla decisione, ma soltanto la natura delle informazioni utilizzate[720]. Lo stesso regime di *disclosure* opera per il caso di azioni sfavorevoli assunte dal datore di lavoro sulla base di informazioni contenute in *consumer reports*. L'unica differenza, infatti, è rinvenibile nella subordinazione dell'accesso al fascicolo del consumatore al suo previo consenso[721].

Al contrario, affinità sussistono nella previsione di un diritto ad accedere alle informazioni e contestarne l'accuratezza. A questo ultimo riguardo, tuttavia, sebbene il

[716] 15 U.S.C.A. § 1681g (g) (1)(C).
[717] 15 U.S.C.A. § 1681g (g)(B).
[718] Ai sensi del FCRA ammontano ad *adverse actions* attività quali "(i) *a denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance*; (ii) *a denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee*; (iii) *a denial or cancellation of, an increase in any charge for, or any other adverse or unfavorable change in the terms of, any license or benefit described in section 1681b(a)(3)(D) of this title*; *and* (iv) *an action taken or determination that is (I) made in connection with an application that was made by, or a transaction that was initiated by, any consumer, or in connection with a review of an account under section 1681b(a)(3)(F)(ii) of this title*; *and (II) adverse to the interests of the consumer*." 15 USCA § 1681a (k).
[719] 15 U.S.C.A. § 1681m (a).
[720] 15 U.S.C.A. § 1681m (b)(1).
[721] 15 U.S.C. § 1681a (k).

FCRA offra ai consumatori una ampia pletora di strumenti per censurare e sanare eventuali erroneità dei dati confluiti nei propri *consumer reports*, tali diritti riguardano pur sempre i dati sulla base dei quali la decisione è stata assunta e non la decisione stessa[722].

3.6.2. I doveri di adverse action notice dell'Equal Credit Opportunity Act

Un regime esplicativo parzialmente più "significativo" è rinvenibile nell'*Equal Credit Opportunity Act* (ECOA)[723], adottato nel 1974 al fine di rimuovere gli ostacoli emersi nella concessione di finanziamenti a clienti di sesso femminile. Con la riforma del 1976 la portata della disciplina antidiscriminatoria è stata estesa in modo tale da fissare il divieto "*for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction*: (1) *on the basis of race, color, religion, national origin, sex or marital status, or age (provided the applicant has the capacity to contract)*; (2) *because all or part of the applicant's income derives from any public assistance program*; or (3) *because the applicant has in good faith exercised any right under this chapter*[724]*."*

Al fine di provare una tale condotta il consumatore (genericamente definito come un "individuo" e quindi inteso in senso sensibilmente diverso dall'accezione eurounitaria) deve dimostrare di aver subito un trattamento diverso in ragione di proprie caratteristiche rientranti in categorie di informazioni protette (*disparate treatment*), ovvero di essere stato sottoposto a pratiche commerciali apparentemente neutrali ma che, a livello diffuso, producono un "*disproportionate adverse effect* […] *on a protected class, unless those practices or policies further a legitimate business need that cannot reasonably be achieved by means that have less disparate an impact*" (c.d. *disparate impact*)[725]. Tale seconda dottrina, peraltro, è frutto di una tendenza a contrastare soluzioni discriminatorie

[722] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 75.

[723] Cfr. J. H. MATHESON, The Equal Credit Opportunity Act: A Functional Failure, 21, *Harv. J. On Legis.*, 1984, 371, 388.

[724] Così 15 USCA § 1691 (a).

[725] *Big Data: A Tool For Inclusion Or Exclusion? Understanding the Issues* (FEDERAL TRADE COMMISSION, 2016), 19 richiamato da V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev.*, 2018, 1707, 1724.

attraverso l'imposizione di obblighi di trasparenza mostrata dalla giurisprudenza già prima dell'adozione dell'ECOA. In particolare, nel caso *Griggs v. Duke Power Co*.[726] la Corte Suprema elaborò una nozione di c.d. "*disparate impact*" sostanzialmente affine a quella discriminazione indiretta che l'articolo 2 para 1 (b) Direttiva 2006/54/CE definisce come una "situazione nella quale una disposizione, un criterio o una prassi apparentemente neutri possono mettere in una situazione di particolare svantaggio le persone di un determinato sesso, rispetto a persone dell'altro sesso, a meno che detta disposizione, criterio o prassi siano oggettivamente giustificati da una finalità legittima e i mezzi impiegati per il suo conseguimento siano appropriati e necessari[727]."

Ciononostante, la complessità dei sistemi automatizzati di *credit reporting* alimentati da *Big Data* aggrava notevolmente le già notorie difficoltà di assolvimento dell'onere probatorio imposto per doglianze fondate sulla dottrina del *disparate impact* e, più in generale, le difficoltà legate alla ricostruzione della logica seguita dalla macchina per valutare il proprio merito creditizio[728].

Non sorprende quindi che, analogamente al FCRA, anche l'ECOA abbia disciplinato specifici doveri informativi per il caso di *adverse actions* che, però,

[726] *Griggs v. Duke Power Co*. 401 U.S. 424 (1971).

[727] La dottrina venne poi ripresa nel caso *McDonnell Douglas Corp. v. Green* 411 U.S. 792 (1973). Cfr. O.C.A. JOHNSON, The Agency Roots of Disparate Impact, 49, *Harvard Civil Rights-Civil Liberties Law Review*, 2014, 125, 140. Per riflessioni sulla c.d. "trappola probatoria" del *disparate impact* si veda quanto scritto da R.A. PRIMUS, Equal Protection and Disparate Impact: Round Three, 117, *Harv. L. Rev*., 2003, 494, 518-21. Cfr. C. FAVILLI, *La nozione di discriminazione tra normativa comunitaria e leggi italiane*, in G. DE MARZO (a cura di), *Il codice delle pari opportunità*, Giuffré editore, Milano, 2007, 147. Sebbene tale teoria non sia espressamente disciplinata dall'ECOA, il prevalente orientamento giurisprudenziale tende ad estenderne esegeticamente il campo d'azione, come avvenuto in *Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc*. con riguardo al *Fair Housing Act*. Il caso concerneva un sistema di assegnazione di crediti d'imposta a costruttori di edilizia popolare, il cui funzionamento era stato accusato di produrre un'iniqua ripartizione del beneficio fiscale sbilanciata a favore di quartieri e comunità prevalentemente abitate da afro-americani. Nonostante il silenzio della normativa in punto di discriminazione indiretta, la Corte ritenne il principio operante e la doglianza fondata in virtù del richiamo alla *ratio decidendi* inaugurata in *Griggs v. Duke Power Co*. *Texas Dep't of Hous. & Cmty. Affairs v. Inclusive Cmtys. Project, Inc*., 135 S. Ct. 2507, 2518 (2015). Cfr. A.D. SELBST, S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1105.

[728] Sulla forte incidenza che la difficoltà di reperire evidenze statistiche e la difformità di orientamenti giurisprudenziali ha avuto sullo scarso successo di azioni fondate sulla dottrina del *disparate impact* si veda quanto osservato da J.L. PERESIE, Toward a Coherent Test for Disparate Impact Discrimination, 84, *Indiana L.J*., 2009, 773, 774-75. Cfr. V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1724-1725; J. BRILL, *The intersection of Privacy and Consumer Protection*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018, 355ss; I.S. RUBINSTEIN, R.D. LEE, P.M. SCHWARTZ, Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 *U. Chi. L. Rev*., 2008, 261, 262-70; T.Z. ZARSKY, Governmental Data Mining and Its Alternatives, 116, *Penn St. L. Rev*., 2011, 285, 295-97.

presentano un ambito materiale di applicazione più ristretto operando soltanto rispetto a dinieghi o modifiche sfavorevoli delle condizioni di finanziamento[729]. Restano quindi escluse tutte quelle misure sfavorevoli che, essendo assunte in ambito assicurativo o lavorativo, sono invece assoggettate ai descritti doveri informativi di cui al FCRA[730].

Dal punto di vista contenutistico, invece, il regime di *disclosure* fissato dall'ECOA sembrerebbe raggiungere dei livelli di significatività più affini a quelli del GDPR. A differenza di quanto visto rispetto al FCRA, infatti, i doveri informativi innescati dalle azioni sfavorevoli disciplinate dall'ECOA implicano non soltanto l'accesso al *credit score* o la conoscenza dei principali fattori che hanno portato all'adozione dello specifico punteggio sul quale, a sua volta, è stata fondata la decisione sfavorevole, ma anche la divulgazione delle specifiche ragioni alla base di quest'ultima[731]. In particolare, il legislatore ha puntualizzato che il finanziatore può assolvere tale dovere fornendo direttamente una siffatta spiegazione, ovvero informando il consumatore del suo diritto a richiederla entro sessanta giorni dalla notifica della *adverse action* assunta nei suoi confronti[732].

A differenza di quanto concluso in sede di analisi della disciplina del FCRA, quindi, nell'ECOA è possibile individuare un diritto ad ottenere una spiegazione che, seppure limitatamente alle sole decisioni sfavorevoli assunte in ambito creditizio, si mostra astrattamente equiparabile a quello disciplinato dal GDPR.

---

[729] Più specificatamente, ai sensi dell'ECOA una *adverse action* è definita come "*a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the amount or on substantially the terms requested" mentre non include "a refusal to extend additional credit under an existing credit arrangement where the applicant is delinquent or otherwise in default, or where such additional credit would exceed a previously established credit limit*." 15 USC § 1691(d)(6).

[730] Per riflessioni circa il carattere più ampio della nozione di *adverse action* di cui al FCRA si veda *Treadway v. Gateway Chevrolet Oldsmobile Inc*., 362 F.3d 971, 982 (7th Cir. 2004).

[731] La *ratio* sottesa al rafforzamento del regime di *disclosure* disciplinato dall'ECOA è rinvenibile non soltanto nell'esigenza di introdurre un grado di trasparenza dei processi decisionali sufficiente a disincentivare condotte discriminatorie dei finanziatori, ma anche a consentire ai clienti di conoscere i fattori che hanno inciso negativamente sul proprio merito creditizio potendo così orientare più consapevolmente la propria condotta futura. Così S. Rep. No. 94-589 (1976), 4 citato da G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 80. Cfr. W.F. TAYLOR, Meeting the Equal Credit Opportunity Act's Specificity Requirement: Judgmental and Statistical Scoring Systems, 29 *Buff. L. Rev*., 1980, 73, 82; C. COGLIANESE, D. LEHR, Transparency and Algorithmic Governance, 71 *Admin. L. Rev*., 2019, 1ss.

[732] 15 U.S.C.A. § 1691 (d)(2).

Tale considerazione sembrerebbe ulteriormente confermata dalle precisazioni offerte dalla Federal Reserve nel Regulation B che, integrando la disciplina dell'ECOA, ha chiarito come, da un lato, la descrizione debba essere specifica ed indicare i motivi principali alla base dell'*adverse action*; mentre, dall'altro, la mera affermazione dell'imputabilità dell'esito del processo di valutazione del merito creditizio al rispetto delle politiche o degli standard interni del finanziatore, ovvero al mancato raggiungimento di un *credit score* adeguato, non rispetti il summenzionato canone di specificità. A tal proposito, nell'allegato C del regolamento sono stati elaborati dei formati standard di c.d. *adverse notification* nei quali è la Parte Prima, denominata "*Principal Reason*(*s*) *for Credit Denial, Termination, or Other Action Taken Concerning Credit*" elenca, a titolo meramente esemplificativo, ventiquattro "*reason codes*" recanti fattori quali: l'impossibilità di verificare le referenze creditizie, la durata dell'impiego, l'insufficienza della retribuzione rispetto all'importo chiesto in prestito, la mancanza di una storia creditizia, il numero di richieste di finanziamento recenti presenti nel proprio "*credit bureau report*"[733]. Inoltre, la Parte II, recante indicazioni circa la "*Disclosure of Use of Information Obtained From an Outside Source*" specifica che, nel caso in cui la decisione sia basata in tutto o in parte su informazioni ottenute da una *consumer reporting agency*, il cliente ha il diritto di rivolgersi alla stessa per conoscere le informazioni contenute nel proprio *credit file*, inclusi i principali fattori che hanno inciso negativamente sul proprio *credit score*[734].

Ad una più attenta lettura, tuttavia, emerge come la finalità antidiscriminatoria perseguita con l'adozione dell'ECOA[735] sia stata in parte declinata in obblighi motivazionali delle decisioni assunte in ambito finanziario da adempiere attraverso modelli esplicativi che, pur indicando le variabili prese in considerazione, tendono ad omettere descrizioni del rapporto (*rectius* la logica) che lega queste ultime alla decisione finale. Come chiarito dallo stesso *Consumer Financial Protection Bureau* (CFPB), infatti, "[*a*] *creditor need not describe how or why a factor adversely affected an applicant. For example, the notice may say 'length of residence' rather than 'too short a period of*

[733] A.D. SELBST, S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1101. Cfr. T.B. GILLIS, J.L. SPIESS, *Big Data* and Discrimination, 86, *U. Chi. L. Rev*., 2019, 459ss.

[734] 12 C.F.R. Pt. 1002, App. C.

[735] Come espressamente chiarito, infatti, "*only if creditors know they must explain their decisions will they effectively be discouraged from discriminatory practices*." Così S. REP. NO. 94-589, 1976, 4.

residence[736]*."* Lo stesso CFPB, peraltro, nell'elaborare dei formulari standard per l'assolvimento dei doveri di *adverse notification*, ha precisato che, ove l'azione sfavorevole sia basata unicamente su un *credit score*, il finanziatore è tenuto a divulgare tutte le variabili prese in considerazione dal sistema di calcolo "*even if the relationship of that factor to predicting creditworthiness may not be clear to the applicant*[737]*."*

Come chiaramente messo in luce da Paul Ohm, infatti, "[*w*]e *are embarking on the age of the impossible-to-understand reason, when marketers will know which style of shoe to advertise to us online based on the type of fruit we most often eat for breakfast, or when the police know which group in a public park is most likely to do mischief based on the way they do their hair or how far from one another they walk*[738]*."* Ciò che rileva, quindi, non è tanto l'esistenza o la complessità della relazione statistica, che potrebbe essere conosciuta e comprensibile, ma della logica sottostante il rapporto pseudo-causale creato dalla macchina tra variabili che, alla coscienza e mente umana, potrebbero apparire completamente indipendenti e slegate le une dalle altre[739].

Ne consegue che, pur essendo rinvenibile nell'ECOA un diritto ad una spiegazione della decisione assunta, quest'ultima potrebbe non risultare significativa (e quindi non equivalente al livello di tutela *ex* artt. 13-15 e 22 GDPR) nella misura in cui venisse a tradursi in una descrizione dei soli fattori che si sono rivelati rilevanti ai fini della decisione (c.d. *outcome-based explanation*), e non anche del peso relativo da ciascuno di essi esercitato sulla stessa (c.d. *logic-based explanation*)[740].

A ulteriore conferma del carattere sostanzialmente non equivalente della *disclosure* disciplinata dall'ECOA si richiama la limitazione dei fattori suscettibili di

[736] Interpretazione ufficiale del Regolamento B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(3) citato da G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 82.

[737] *Official Interpretations of Reg. B*, 12 C.F. RCFR. pt. 1002, supp. I, § 1002.9(b)(2) §§ 4-5.

[738] Così P. OHM, The Fourth Amendment in a World Without Privacy, 81, *Miss. L.J.*, 2012, 1309, 1318, citato da A.D. SELBST, S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1096. Per riflessioni sulle difficoltà di ricostruire la causalità nella logica algoritmica seguita nel compiere processi decisionali automatizzati per la frequente assenza di vincoli di causa-effetto tra fattori presi in considerazione dalla macchina e le decisioni raggiunte si veda Y. BATHAEE, The Artificial Intelligence Black Box and the Failure of Intent and Causation, 31, *Harv. J.L. & Tech*., 2018, 889ss.

[739] Cfr. J. GRIMMELMANN, D. WESTREICH, Incomprehensible Discrimination, 7, *Calif. L. Rev. Online*, 2016, 164, 173.

[740] A.D. SELBST, S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1099-1100.

confluire in una *adverse notification* che il Federal Reserve Board, al fine di contenere fenomeni di c.d. *overinformation* e preservare l'utilità delle spiegazioni fornite, ha ridotto ad un massimo di quattro[741]. Come correttamente notato in dottrina, tuttavia, tale approccio, per quanto apprezzabile nelle intenzioni, non può che rivelarsi fallimentare ogni qualvolta il sistema da descrivere risulti particolarmente complesso, potendo offrire soltanto descrizioni parziali e quindi non soltanto non significative ma anche scarsamente educative[742].

Se, peraltro, a tale limite si aggiunge il carattere materialmente e soggettivamente limitato della disciplina dettata dal FCRA, così come dall'ECOA, nonché l'adozione di una nozione di dato personale che, a differenza di quella definita nell'articolo 4 GDPR, esclude informazioni solo indirettamente riconducibili ad una persona fisica[743], si rende evidente il carattere a dir poco limitato, se non del tutto illusorio delle tutele ivi apprestate. Soprattutto nel contesto *Big Data*, infatti, caratterizzato dalla assoluta atipicità e varietà delle informazioni utilizzabili, nonché dalla costante emersione di nuovi soggetti e modelli di business, aggirare le tutele predisposte dal FCRA e dall'ECOA è particolarmente agevole, essendo sufficiente, ad esempio, che il finanziatore raccolga e

[741] 12 C.F.R. pt. 1002 supp. I, para. 9(b)(2) (2018).

[742] Parte della dottrina ha tentato di sopperire alle lacune in punto di logica delle spiegazioni *output-based* teorizzandone una declinazione c.d. *post hoc* consistente in rappresentazioni semplificate del concreto funzionamento di processi decisionali molto più complessi realizzate modificando il valore di un singolo fattore in modo tale che, lasciando invariato il valore degli altri, il delta della variazione sia indicativo del peso relativo esercitato dalla variabile modificata sul risultato finale. Siffatto modello di spiegazione, tuttavia, omettendo informazioni sulla logica complessivamente seguita nel processo decisionale, rischia di risultare ingannevole per i clienti. Questi ultimi, infatti, potrebbero essere indotti a presumere che le variabili abbiano esercitato lo stesso peso nei processi decisionali che coinvolgono altri soggetti, rendendo così imprevedibile il modello e scarsamente educativa la spiegazione. A.D. SELBST, S. BAROCAS, The Intuitive Appeal of Explainable Machines, cit., 1104 e 1115. Cfr. A. DATTA, S. SEN, Y. ZICK, *Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems* (PROCEEDINGS OF THE 2016 IEEE SYMPOSIUM ON SECURITY & PRIVACY), 598; A. HENELIUS *et al.*, A Peek into the Black Box: Exploring Classifiers by Randomization, 28, *Data Mining & Knowledge Discovery*, 2014, 1503ss.

[743] In particolare, gli indirizzi IP e le altre tipologie di identificativi unici soltanto indirettamente riconducibili ad una persona fisica identificata sono soggetti ad uno status giuridico differenziato e, specialmente negli Stati Uniti, spiccatamente ambiguo. Se, infatti, tali tipologie di informazioni rientrano nella nozione eurounitaria di dato personale e sono quindi sottoposti alle tutele del GDPR, l'ordinamento (*rectius* la dottrina) statunitense tende ad assimilarli a *Non Personally-Identifiable Information*. J. BARRETT GLASGOW, *Data Brokers: Should They Be Reviled or Revered?*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2018, 26.

tratti i dati internamente, senza avvalersi di una CRA, per collocarsi al di fuori del raggio d'azione della normativa[744].

In conclusione, il diritto di ottenere l'intervento umano, di esprimere la propria opinione, così come il diritto ad ottenere una spiegazione (*rectius* informazioni significative) relativamente alla logica utilizzata nel processo decisionale (automatizzato o meno) non sembrerebbero trovare equivalenti nel FCRA o nell'ECOA.

3.7. Il *due process* come limite alla legittimità di processi decisionali automatizzati "opachi"

A dispetto di quanto l'esclusiva attenzione al settore finanziario prestata dall'ECOA potrebbe far pensare, il legislatore statunitense si è premurato di estendere un analogo regime anche in altri ambiti attraverso una serie di interventi normativi che, per quanto settoriali[745], perseguono una comune finalità antidiscriminatoria e vengono perciò complessivamente ricompresi nella più generica nozione di *equal protection laws*. La sempre più frequente automatizzazione di processi decisionali altamente sensibili, infatti, come quelli condotti in ambito lavorativo per la selezione del personale[746], ha reso particolarmente pressante l'esigenza di contemperarne gli effetti potenzialmente discriminatori[747].

Ciononostante, la mancata riproduzione di istituti analoghi a quello dell'*adverse action notice* al di fuori dell'ambito di applicazione dell'ECOA ha fatto sì che, nei settori estranei a quello del credito, gli strumenti di reazione avverso condotte discriminatorie

[744] V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1729. Cfr. J. ADEBAYO, M. HURLEY, Credit Scoring in the Era of *Big Data*, 18, *Yale J.L. & Tech*., 2016, 148, 186.

[745] Per riflessioni sulla disciplina antidiscriminatoria dettata nel settore del mercato immobiliare dal *Fair Housing Act* si veda, fra gli altri, *A Primer on Fair Housing Law* (FAIR HOUSING LEGAL SUPPORT CENTER AND CLINIC, John Marshall Law School, 2014), 16. Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 86-87 e 93.

[746] Le fonti principali in punto contrasto alle condotte discriminatorie dei datori di lavoro sono il Titolo VII del *Civil Rights Act*, nonché l'*Age Discrimination in Employment Act.* Cfr. P. KIM, Data-Driven Discrimination at Work, 58, *Wm. & Mary L. Rev*., 2017, 857, 861-62.

[747] Così GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, adottate il 3 ottobre 2017 (versione emendata e adottata il 6 febbraio 2018) (WP 251 rev.01), 23.

venissero a fondarsi esclusivamente sul summenzionato regime del *disparate impact*[748]. Quest'ultimo, tuttavia, ammettendo la discriminazione indiretta prodotta da pratiche commerciali giustificate da legittime esigenze di business non altrettanto efficacemente perseguibili con prassi alternative[749], rende tale istituto spesso inadeguato a neutralizzate decisioni che, come nel caso delle assunzioni, danno rilievo a requisiti che, pur se discriminatori, rispondono a specifiche esigenze del datore di lavoro[750].

Recente giurisprudenza, tuttavia, ha messo in evidenza come tale carenza di effettività possa essere, almeno in parte, sanata sfruttando la capacità dei vincoli procedurali della *due process clause* di infondere maggiore equità e trasparenza nei processi decisionali automatizzati[751]. In senso analogo si è espressa anche la dottrina che, nell'analizzare le tipologie di danno potenzialmente derivanti da processi decisionali unicamente automatizzati[752], ha osservato come l'impossibilità di conoscere il percorso logico seguito dalla macchina per addivenire ad una decisione poi rivelatasi dannosa (ad esempio perché erronea o discriminatoria) non integrerebbe gli estremi di un danno alla privacy ma del *due process*[753].

Prima di entrare nel merito dell'episodio giurisprudenziale, si ricorda che negli Stati Uniti il principio del giusto processo è tradizionalmente ricondotto al dettato del Quinto e del Quattordicesimo emendamento. In particolare, quest'ultimo, ratificato nel 1868, vieta agli Stati di privare le persone della propria vita, libertà o proprietà senza un giusto processo di legge[754]. Inizialmente declinato in prospettiva squisitamente formale e procedimentale, a partire dal caso *Griswold v. Connecticut*[755] si è arricchito di una

[748] Per una più approfondita disamina dell'istituto si veda quanto osservato *supra sub* §3.6.2.

[749] 29 CFR § 1607.3

[750] Cfr. S. HOFFMAN, *Big Data* and the Americans with Disabilities Act, 68, *Hastings L.J.*, 2017, 777, 779.

[751] G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 90.

[752] M.R. CALO, The Boundaries of Privacy Harm, 86, *Ind. L.J.*, 2011, 1131, 1146-52.

[753] D. KEATS CITROW, Technological Due Process, 85, *Wash UL Rev*, 2008, 1249ss.

[754] Insieme al Tredicesimo emendamento, volto ad abolire la schiavitù, e al Quindicesimo emendamento, volto a estendere il diritto di voto agli Afro-americani, il Quattordicesimo emendamento fa parte del trittico normativo noto come *Reconstruction Amendments*, introdotto all'indomani della guerra di secessione. Cfr. K. LEIGH, *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015, 10.

[755] Furono i giudici White e Marshall Harlan II ad aprire la strada alla c.d. *substantial due process clause*. In particolare, nel recepire quanto già sostenuto qualche anno prima da Harlan nella sua *dissenting opinion* nel caso *Poe v. Ullman* (1961), i due giudici sostennero l'idea per cui la *due process clause* di cui

accezione sostanziale volta ad assicurare che nessun procedimento, per quanto insindacabile dal punto di vista formale, possa incidere, dal punto di vista sostanziale, sul nocciolo duro e intangibile delle libertà individuali, seppure "innominate" perché non esplicitamente enumerate nel *Bill of Rights*[756].

Tale precedente venne poi più volte ripreso nel percorso giurisprudenziale di affermazione della menzionata declinazione "decisionale" della nozione statunitense di privacy[757], generalmente riguardata come privacy della mente[758] o, nelle parole di Mill,

---

al Quattordicesimo emendamento si declini in una duplice versione: una processuale e una sostanziale. Se la prima assume una prospettiva formale e guarda al rispetto di garanzie procedurali volte ad assicurare l'uguaglianza di fronte alla legge, la seconda guarda all'esigenza di offrire tutela ad una pletora di diritti atipici ed innominati, ma cionondimeno essenziali al mantenimento delle libertà fondamentali che devono essere sempre rispettate, anche a fronte di procedimenti formalmente impeccabili. Cfr. K.L. HALL e J.J. PATRICK, *The Pursuit of Justice. Supreme Court Decisions that Shaped America*, Oxford, Oxford University Press, 2006, 153.

[756] M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 27.

[757] In particolare, tra le sentenze all'origine del concetto di *decisional privacy* si richiamano quelle adottate in occasione del caso *Roe v. Wade* (410 U.S. 113, 1973) in cui nel valutare la legittimità di una legislazione che vietava l'aborto in mancanza di problemi di salute della donna, la Corte Suprema riepilogò i passaggi giurisprudenziali più salienti del percorso di affermazione della privacy, chiarendone la portata. In particolare, nelle parole del giudice Blackmun: "*[t]he Constitution does not explicitly mention any right of privacy. In a line of decisions, however, going back perhaps as far as* Union Pacific R. Co. v. Botsford, *141 U.S. 250, 251 (1891), the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First Amendment,* Stanley v. Georgia, *394 U.S. 557, 564 (1969); in the Fourth and Fifth Amendments,* Terry v. Ohio, *392 U.S. 1, 8-9 (1968),* Katz v. United States, *389 U.S. 347, 350 (1967),* Boyd v. United States, *116 U.S. 616 (1886), see* Olmstead v. United States, *277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); in the penumbras of the Bill of Rights,* Griswold v. Connecticut, *381 U.S. at 484-485; in the Ninth Amendment, id. at 486 (Goldberg, J., concurring); or in the concept of liberty guaranteed by the first section of the Fourteenth Amendment, see* Meyer v. Nebraska, *262 U.S. 390, 399 (1923). These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty,"* Palko v. Connecticut, *302 U.S. 319, 325 (1937), are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage,* Loving v. Virginia, *388 U.S. 1, 12 (1967); procreation,* Skinner v. Oklahoma, *316 U.S. 535, 541-542 (1942); contraception,* Eisenstadt v. Baird, *405 U.S. at 453-454; id. at 460, 463-465 (White, J., concurring in result); family relationships,* Prince v. Massachusetts, *321 U.S. 158, 166 (1944); and childrearing and education,* Pierce v. Society of Sisters, *268 U.S. 510, 535 (1925),* Meyer v. Nebraska, supra. *This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy." Roe v. Wade* (410 U.S. 113, 1973), 152-154. Importante fu anche il ruolo della pronuncia in *Planned Parenthood of Central Missouri v. Danforth* (428 US 52, 1976), dove richiamando i principi affermati in *Roe v. Wade*, la Corte sancì l'illegittimità della previsione per cui l'aborto potesse essere eseguito soltanto ove al consenso della donna si associassero anche il consenso del marito o dei genitori della stessa, ove minorenne. Cfr. B.A. BRODY, *Abortion and the Law*, in J.M. HUMBER e R.F. ALMEDER (a cura di), *Biomedical Ethics and the Law*, II ed., Berlino, Springer, 45 ss. Cfr. W. FREEDMAN, *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987, 4.

[758] M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 24. Sul concetto di privacy intellettuale si veda N.M. RICHARDS, Intellectual Privacy, 87, *Text.L. Rev*., 2008, 387 ss.

come la "*liberty of tastes and pursuits*"[759], ovvero la libertà di formare liberamente le proprie opinioni, credenze e moralità, conformandovi il proprio stile di vita[760]. Libertà questa, strumentale e indispensabile a contrastare quella che è stata efficacemente definita come la "tirannia delle norme sociali e dell'opinione maggioritaria"[761].

Tornando al ruolo che tale principio può assumere nel contrasto agli effetti discriminatori insiti nei processi decisionali automatizzati, un chiaro esempio giurisprudenziale è offerto dal caso *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist.*[762], avente ad oggetto la decisione del distretto scolastico di Houston di licenziare tutti gli insegnanti a cui un software privato di *Educational Value–Added Assessment* aveva attribuito un punteggio inferiore ad una certa soglia. Gli insegnanti, lamentando la violazione del principio del contraddittorio per effetto dell'impossibilità di accedere all'algoritmo utilizzato, impugnarono i licenziamenti. La Corte accolse le doglianze degli attori osservando come l'utilizzo da parte di un ente pubblico di un algoritmo "segreto" (*rectius* coperto da diritti di proprietà intellettuale) per prendere "*high stakes employment decisions*" fosse incompatibile con i principi base del giusto processo. Ciò in quanto, l'impossibilità di accedere alla formula tecnico-matematica implementata dal software così come alle informazioni dallo stesso utilizzate, impediva agli interessati di verificare e, eventualmente, contestare la correttezza della decisione, con conseguente sacrificio dell'effettività del contraddittorio e, più in generale, del loro diritto ad un giusto processo[763].

Tale conclusione non può che rievocare le analoghe considerazioni svolte in Italia dal Consiglio di Stato, il quale, posto di fronte a simili scelte di automazione del processo decisionale amministrativo, ha in più occasioni ribadito come l'impossibilità di

[759] Cfr. C.L. TEN, Mill's *On Liberty.A Critical Guide*, Cambridge, Cambridge University Press, 2009.

[760] Il professore Louis Henkin sottolinea come "[*p*]*rimarily and principally the new Right of Privacy is a zone of prima facie autonomy, of presumptive immunity from regulation, in addition to that established by the First Amendment.*" ID., Privacy and Autonomy, 74, *Columbia L. Rev*, 1974, 1410.

[761] Si parla, in questo senso, di protezione "*against the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them* […]". M. MCTHOMAS, *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013, 25.

[762] *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist*., 251 F. Supp. 3d 1168, 1171 (S.D. Tex. 2017).

[763] Cfr. G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 92.

comprendere le modalità di funzionamento dell'algoritmo costituisca "di per sé un vizio tale da inficiare la procedura". L'esigenza di piena conoscibilità della regola algoritmica, infatti, si configura strumentale a quel pieno sindacato giurisdizionale "declinazione diretta del diritto di difesa del cittadino, al quale non può essere precluso di conoscere le modalità (anche se automatizzate) con le quali è stata in concreto assunta una decisione destinata a ripercuotersi sulla sua sfera giuridica[764]."

Nonostante tale innegabile affinità nell'applicazione esegetica del principio del giusto processo nel contesto dei processi decisionali automatizzati compiuti da pubbliche amministrazioni, la mancanza nell'ordinamento statunitense di diritti informativi equivalenti a quelli disciplinati dal combinato disposto degli articoli 15 e 22 GDPR, ha privato il giudice texano di quella leva normativa che, invece, ha consentito al giudice italiano di stemperare la segretezza dell'algoritmo riconoscendo un diritto di accesso individuale allo stesso in capo ai singoli interessati[765]. L'assenza di un diritto di spiegazione e, quindi, di accesso, con cui bilanciare i diritti di proprietà intellettuale sul software utilizzato a fini decisionali non ha lasciato alla corte statunitense altra soluzione che imporre al distretto scolastico la revoca delle decisioni e l'abbandono della soluzione automatizzata[766].

Emerge quindi come gli standard di trasparenza ed equità che la *due process clause*, seppure limitatamente al settore pubblico, è astrattamente idonea ad instillare nei processi decisionali automatizzati, ove non accompagnati da adeguati diritti di informativi tesi a contemperare le contrapposte esigenze di sfruttamento commerciale del software, siano suscettibili di tradursi in un paradossale e sproporzionato sacrificio delle potenzialità tecnologiche di efficientamento dell'azione amministrativa.

[764] Consiglio di Stato, Sez. VI, Sentenza n. 2270 del 8 aprile 2019; Consiglio di Stato, Sez. VI, Sentenza n. 8472 del 13 dicembre 2019. Cfr. E. PROSPERETTI, Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del TAR Lazio, *Diritto dell'Informazione e dell'Informatica*, 4, 2019, 979 ss; A. CARRATTA, Decisione robotica e valori del processo, *Rivista di diritto processuale*, 2, 2020, 491ss; D.U. GALETTA, Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia, *Rivista Italiana di Diritto Pubblico Comunitario*, 3, 2020, 501 ss; E. FALLETTI, Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, *Diritto dell'informazione e dell'informatica*, 2, 2020, 169ss; E. PELLECCHIA, Profilazione e decisioni automatizzate al tempo della "Black Box Society": qualità dei dati e leggibilità dell'algoritmo nella cornice della "*responsible research and innovation*" in *Le Nuove leggi civili commentate*, 2018, 1209 ss.

[765] TAR Lazio, sez. III-bis, Sentenza n. 3769/2017.

[766] *Houston Fed'n of Teachers v. Houston Indep. Sch. Dist*., 251 F. Supp. 3d 1168, 1179 (S.D. Tex. 2017).

La lacunosa settorialità della legislazione federale sin qui esaminata ha indotto parte della dottrina, così come alcuni legislatori statali, a stimolare una revisione del sistema delle fonti in materia di *data privacy* vigente negli Stati Uniti. Le tre espressioni più paradigmatiche e recenti di tale rinnovata sensibilità verso la necessità di dotarsi un corpo normativo c.d. "*industry-agnostic"* recante norme per la protezione dei dati personali sono il rinnovato interesse dottrinale per un possibile intervento "legislativo" della *Federal Trade Commission*, la recente entrata in vigore del *California Consumer Privacy Act* e l'adozione dei *Data Privacy Principles* da parte dell'*American Law Institute*, ai quali verranno rispettivamente dedicati gli ultimi paragrafi del capitolo[767].

3.8. Il ruolo della Federal Trade Commission in ambito di *data privacy*

In prospettiva di *enforcement*, particolarmente importante è il ruolo progressivamente assunto dalla *Federal Trade Commission* (FTC), la cui azione di vigilanza sul rispetto delle pratiche commerciali scorrette è particolarmente adatta a monitorare l'implementazione di trattamenti di dati da parte del settore privato statunitense che, come visto, opera in contesto di sostanziale de-regolamentazione[768].

Istituita nel 1914 con compiti antitrust, infatti, la FCT vide estendere le proprie competenze nel 1938 quando il c.d. emendamento *Wheeler-Lea* modificò il *Federal Trade Commission Act* integrando il divieto il divieto di "*unfair methods of competition in or affecting commerce*" con quello di "*unfair or deceptive acts or practices in or affecting commerce*"[769]. In tal modo, e su stimolo del Congresso, a partire dalla metà degli anni '90 la FTC iniziò a vigilare e sanzionare violazioni delle dichiarazioni rese nelle privacy policies in quanto integranti gli estremi di condotte ingannevoli ed inique, assurgendo a autorità federale preposta, fra l'altro, alla protezione dei dati dei

[767] V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707, 1735.

[768] Tale competenza, tuttavia, presenta dei limiti, restando escluse gran parte delle agenzie federali e statali, delle organizzazioni non governative e degli enti commerciali operanti nei settori di trasporto, assicurativo, bancario e delle telecomunicazioni. C.N. SKELTON, FTC Data Security Enforcement: Analyzing the Past, Present, and Future, 25, *J. Anti., UCL & Privacy Sec. St. B. Cal*, 2016, 306ss; J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J*., 23, 2019, 23, 26. Cfr. R. GELLMAN e P. DIXON, *Failures of Privacy Self-Regulation in the United States*, in D. WRIGHT e P. DE HERT (a cura di), *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, Law, Governance and Technology Series 25, Springer, 2016, 70ss.

[769] 15 USCA § 45a (1).

consumatori[770]. In particolare, dal 2006 è allo scopo operativa la *Division of Privacy and Identity Protection* precipuamente deputata a monitorare "*cutting-edge consumer privacy matters"* attraverso attività di *enforcement* e *policy-making*[771].

In quest'ottica, le varie leggi federali settoriali recanti norme in materia di protezione dei dati personali sono complessivamente riguardate come componenti di più ampi strumenti normativi di tutela dei consumatori[772]. Allo scopo, il Congresso ha attribuito alla FTC il potere di vigilanza sull'attuazione di una serie di normative settoriali quali il *Controlling the Assoult of Non-Solicited Pornography and Marketing* (CAN-SPAM) *Act*[773], il *Children's Online Privacy Protection Act* (COPPA)[774], nonché l'ECOA e il FCRA[775]. Inoltre, mancando un quadro normativo intersettoriale così come un'Autorità con competenze esclusive in materia di *data privacy*, a seguito della

[770] S. HETCHER, The De Facto Federal Privacy Commission, 19, *J. Marshall J. Computer & Info*. *L*., 2000, 109, 131.

[771] Più specificatamente, la FTC tende ad assimilare l'inadeguatezza degli standard di protezione dei dati personali dei propri clienti, l'inidoneità delle misure di sicurezza e prevenzione di attacchi informatici, ovvero la violazione o modifica delle privacy *policies* senza preavviso alla clientela, a pratiche commerciali ingannevoli e quindi lesive degli interessi dei consumatori, innescando così la propria competenza ai sensi della sezione 5 del *Federal Trade Commission Act*. D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 583, 603; D. KLITOU, *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014, 40. Per più generali riflessioni sulla competenza della FTC in punto di contrasto a pratiche commerciali ingannevoli si veda M. HOFMANN, *Federal Trade Commission Enforcement of Privacy*, in K.J. MATHEWS (a cura di), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, II ed., Practicing Law Institute, 2011, § 4:1.2. Per riflessioni sull'evoluzione diacronica del ruolo della FTC nella vigilanza sul rispetto della disciplina consumeristica si veda A. SERWIN, The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48, *San Diego L. Rev.*, 2'11, 809, 811; J.N. SLOANE, Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J.*, 23, 2019, 23, 26.

[772] Cfr. W. MCGEVERAN, Friending the Privacy Regulators, 58, *Ariz. L. REV*., 2016, 959, 961.

[773] Tale legge regola la raccolta e l'uso di indirizzi mail al fine dell'invio di messaggi elettronici commerciali, ovvero il cui obiettivo principale è pubblicizzare o promuovere prodotti o servizi. La legge impone l'adozione di indirizzi mittenti e oggetti non ingannevoli, nonché la previsione di meccanismi di opt-out per i destinatari e la chiara indicazione della natura pubblicitaria della comunicazione. S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299, 303, 309.

[774] Tale legge regola la raccolta e l'uso di dati personali relativi a utenti minori di tredici anni da parte di gestori di siti internet e di applicazioni per dispositivi mobili ovvero di "*any operator that has actual knowledge that it is collecting personal information from a child*". Nell'ottemperare ai compiti di vigilanza in materia attribuitigli dal Congresso, la FTC nel 2000 ha elaborato la c.d. *Children's Online Privacy Protection Rule* per chiarire gli obblighi di condotta imposti ai titolari del trattamento. Inoltre, nel 2013 la FTC ha interpretato estensivamente la nozione di dati personali fino ad includervi i "*persistent identifiers*", tra cui i *cookies*, utilizzati per riconoscere i dispositivi e seguirli per monitorarne la navigazione in rete. A tal riguardo, la legge impone la richiesta del previo consenso dei genitori, nonché la pubblicazione di privacy *policies* in cui i gestori dei siti *web* specificano le categorie di informazioni raccolte, gli utilizzi delle stesse nonché le categorie di terzi con cui i dati sono condivisi. Dal 2013, anche i giocattoli con connessione alla rete ricadono nell'ambito di applicazione della disciplina, i genitori devono perciò avere il diritto di conoscere i dati raccolti rispetto ai propri figli, nonché il diritto di ottenerne la cancellazione.

[775] S.M. BOYNE, Data Protection in the United States, 66, *Am J Comp L*, 2018, 299, 301.

conclusione del *Safe Harbor Agreement* la FTC si venne a trovare in una posizione assolutamente privilegiata nel panorama istituzionale statunitense e, nonostante l'atipicità delle sue competenze rispetto alle Autorità istituite a livello europeo per la vigilanza in materia di privacy, venne investita dei compiti di monitoraggio sul rispetto del regime transfrontaliero di circolazione dei dati personali[776].

Infine, il più volte menzionato carattere settoriale e lacunoso del quadro normativo federale in materia di *data privacy*, ha finito per conferire un valore sempre più normativo al complesso degli accordi transattivi generalmente conclusi dalla FTC all'esito di azioni di *enforcement*. Le determinazioni così assunte, infatti, informano la condotta degli operatori del settore e, per questo, sono stati qualificati da parte della dottrina come fonte di una c.d. "*new common law of privacy*"[777].

Lo strumento attraverso il quale i provvedimenti della FTC sono assurti a fonte "funzionalmente equivalente" a quella di *common law* è la procedura del *consent order*. Ciò in quanto, il carattere pubblico della procedura, associato all'uniformità degli orientamenti assunti dalla Commissione, hanno reso più prevedibile l'azione di vigilanza della Commissione inducendo gli enti vigilati ad adeguarvi le proprie prassi aziendali[778]. Inoltre, poiché, anche in ragione delle ridotte risorse a disposizione della FTC, la scelta delle condotte da investigare è focalizzata sulle violazioni più macroscopiche ovvero su quelle poste in essere dalle imprese di maggiori dimensioni, in modo tale da rafforzare l'efficacia deterrente e educativa dei provvedimenti[779].

---

[776] R.R. SCHRIVER, You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission, 70, *Fordham L. Rev*., 2002, 2777, 2792; *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (FEDERAL TRADE COMMISSION, 2012), 2.

[777] D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 583. In senso analogo J. HURWITZ, Data Security and the FTC's UnCommon Law, 103, *Iowa L. Rev.*, 2016, 101, 132, 158.

[778] In queso senso D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, 114, *Colum. L. Rev*., cit., 607 spec. nt. 91 ove, richiamando le statuizioni giurisprudenziali avanzate in *United States v. ITT Cont'l Baking Co*., 420 U.S. 223, 238 (1975), sottolineano le affinità che gli effetti dei *consent orders* mostrano con quelli di un contratto. Al contrario, in senso critico si sono espressi G.M. STEGMAIER, W. BARTNICK, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data-Security Requirements, 20, *Geo. Mason L. Rev*., 2013, 673, 676; M.D. SCOTT, The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60, *Admin. L. Rev*., 2008, 127, 130-31. Cfr. A.R. GLUCK, The Federal Common Law of Statutory Interpretation: Erie for the Age of Statutes, 54, *Wm. & Mary L. Rev*., 2013, 753, 757.

[779] Sull'influenza esercitata dagli orientamenti assunti dalla FTC in sede in *enforcement* sull'interpretazione giurisprudenziali della legislazione del settore si vedano le riflessioni di J. BRAUCHER, Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive

Dal punto di vista procedurale, nel caso in cui la FTC abbia motivo di ritenere che sia occorsa una violazione della normativa di sua competenza, può avviare un'investigazione che si conclude con un *complaint* recante indicazioni circa la natura delle irregolarità riscontrate e le azioni rimediali necessarie. Il destinatario del provvedimento può impugnarlo, investendo della questione la corte distrettuale o amministrativa territorialmente competente, ovvero può avviare delle negoziazioni con con la FTC per addivenire ad un c.d. *consent order agreement* attraverso il quale, senza ammettere alcuna responsabilità e rinunciando a qualsiasi diritto di revisione giurisdizionale dell'accordo, vengono individuate le misure da adottare per ripristinare la conformità alla normativa[780].

Dal punto di vista contenutistico, i *consent orders* della FTC generalmente includono una serie piuttosto standardizzata di misure correttive che, accompagnando le sanzioni pecuniarie, mirano a ripristinare un livello adeguato di tutela della *data privacy* dei consumatori interessati. Ne sono esempi: (i) ordini di inibizione delle condotte ritenute illecite[781]; (ii) ordini di notifica alla clientela della violazione rilevata dalla FTC e delle misure organizzative adottate per rimediarvi[782]; (iii) ordini di cancellazione, ovvero di divieto di trattamento, dei dati illecitamente raccolti[783]; (iv) ordini di modifica delle proprie privacy policies al fine di rendere più chiare e comprensibili le modalità di utilizzo dei dati personali[784]; (v) ordini di implementazione di "*comprehensive security programs*" volti a individuare e documentare l'introduzione di salvaguardie

Authority in the Common Law of Fraud, 48, *Ariz. L. Rev*., 2006, 829, 851. Sottolineano, invece, divergenze operative tra gli standard adottati dale Corti e dalla FTC in punto di vigilanza sul rispetto della disciplina consumeristica H.N. BUTLER, J.D. WRIGHT, Are State Consumer Protection Acts Really Little-FTC Acts?, 63, *Fla. L. Rev*., 2011, 163, 182-88.

[780] Tali *settlement orders* sono vincolanti per le parti e in, caso di violazione, comportano il pagamento di penali fino a sedicimila dollari per singola violazione, nonché eventuali ulteriori ristori valutati su base equitativa dal giudice distrettuale. Da notare, come la sezione quinta del *FTC Act* non riconosca legittimazione attiva in capo ai singoli interessati, ma ammetta l'avvio di procedimenti amministrativi solo da parte della Commissione. D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 611.

[781] Come avvenuto, *ex multis*, in *In re Lookout Servs., Inc*., 151 F.T.C. 532, 536-37, 539 (2011); *In re US Search, Inc*., 151 F.T.C. 184, 187-88, 190 (2011); *United States v. Am. United Mortg*. Co., No. 07C 7064, at 5 (N.D. Ill. Dec. 18, 2007); *In re Twitter, Inc.*, FTC File No. 092 3093, No. C-4316 (2011); *In re Directors Desk, LLC*, FTC File No. 092 3140, No. C-4281 (2010); etc.

[782] Ad esempio, *FTC v. Frostwire, LLC*, No. 11-cv-23643-CV-GRAHAM, at 13-16 (S.D. Fla. Oct. 12, 2011).

[783] Così, ad esempio, *United States v. Artist Arena, LLC*, No. 1:12-cv-07386-JGK, at 4 (S.D.N.Y. Oct. 3, 2012) e *In re Aspen Way Enters., Inc*., FTC File No. 112 3151, No. C-4392, at 6 (F.T.C. Sept. 25, 2012).

[784] E.g. *United States v. Sony BMG Music Entm't*, No. 08 Civ. 10730 (LAK), at 4-5 (S.D.N.Y. Dec. 15, 2008); Warner-Lambert Co. v. FTC, 562 F.2d 749, 763-64 (D.C. Cir. 1977).

amministrative, tecniche e fisiche proporzionali alle dimensioni e alla complessità dell'attività svolta dal titolare del trattamento[785]; (vi) ordini di implementazione di "*comprehensive privacy programs*" volti a individuare, monitorare e risolvere eventuali lacune nel regime aziendale di protezione dei dati[786]; (viii) ordini di sottoposizione a verifiche biennali di esperti indipendenti sul rispetto dei *consent orders*[787]*;* nonché (ix) obblighi di notifica di eventi potenzialmente idonei ad incidere sull'assetto organizzativo del titolare con conseguenti ripercussioni sul rispetto delle misure imposte dalla FTC[788].

Spostando l'attenzione sul versante sostanziale, le condotte sanzionate dalla FTC sono raggruppabili in tre macrocategorie: *deception*, *unfairness* e, prima della sua invalidazione, rispetto del *Privacy Shield agreement*[789].

La *deception* rappresenta il più risalente ambito di intervento della FTC che, radicando la propria competenza sulla sezione quinta del *FTC Act*, mira a reprimere false rappresentazioni, omissioni o qualsiasi altra pratica ingannevole che induca il consumatore ad agire in modo a sé pregiudizievole. La prima e principale categoria di condotte tradizionalmente ascritte all'istituto della *deception* è quella della "*broken promise of privacy*", integrata ogni qualvolta siano posti in essere trattamenti dei dati degli utenti difformi alle dichiarazioni rese nelle *privacy policies* del servizio[790].

Tale fattispecie, peraltro, svolge un ruolo importante anche in materia di processi decisionali automatizzati, consentendo alla FTC di rafforzare i doveri di chiarezza e trasparenza in capo ai soggetti vigilati. Ad esempio, nel caso CompuCredit la

[785] *In re HTC Am. Inc*., FTC File No. 122 3049, No. C-4406, at 5 (F.T.C. July 2, 2013).
[786] *In re Google Inc*., FTC File No. 102 3136, No. C-4336, at 4 (F.T.C. Oct. 13, 2011).
[787] *In re HTC Am. Inc*., FTC File No. 122 3049, No. C-4406, at 5 (F.T.C. July 2, 2013).
[788] Cfr. D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 619.
[789] R.R. SCHRIVER, You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission, 70, *Fordham L. Rev.*, 2002, 2777ss.
K.A. BAMBERGER, D.K. MULLIGAN, Privacy on the Books and on the Ground, 63, *Stan. L. Rev*., 2011, 247, 313. Cfr. *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies* (FEDERAL TRADE COMMISSION, 2012); *Mobile Privacy Disclosures: Building Trust Through Transparency* (FEDERAL TRADE COMMISSION, 2013); *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (FEDERAL TRADE COMMISSION, 2012), 2.
[790] Le tipologie più frequenti di promesse riguardano l'impegno a: (i) non trasmettere i dati a terzi; (ii) raccogliere solo categorie di informazioni indicate nelle privacy policies; (iii) mantenere l'anonimato; (iv) adottare adeguate misure di sicurezza; e (v) non vendere i dati personali raccolti nell'ambito di procedure fallimentari. Ad esempio, in *In re Eli Lilly & Co.*, 133 F.T.C. 763, 767 (2002) la FTC ritenne che l'inadeguatezza delle procedure predisposte per la formazione dei propri dipendenti in materia di trattamento dei dati, pubblicizzate nelle proprie *privacy policies*, integrasse gli estremi di una pratica commerciale ingannevole. Cfr. D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 629.

Commissione ha qualificato come ingannevole la condotta di tale società di marketing per carte di credito che, nel pubblicizzare la possibilità dei clienti di avvalersi di estensioni del plafond della carta, aveva omesso di informarli che, al contrario, per effetto dell'utilizzo di un modello di *behavioral scoring*, la linea di credito sarebbe stata invece ridotta a fronte di alcune categorie di spese quali, ad esempio, quelle effettuate presso consulenti matrimoniali, nightclubs, banchi dei pegni e saloni di bellezza[791].

Inoltre, progressiva importanza è stata assunta dalle ipotesi di mancata implementazione dei livelli di *data security* pubblicizzati e promessi ai propri utenti. A tal riguardo, infatti, l'analisi diacronica della "giurisprudenza" della FTC mostra una propensione a definire con crescente specificità lo standard delle "*reasonable security measures*"[792]. Ad esempio, nel recente caso *FTC v. Wyndham Worldwide Corp*. la Commissione non si è limitata a rilevare l'inadeguatezza dell'infrastruttura di *cybersecurity* ma, nell'individuare le principali falle del sistema, e ispirandosi alle *best practices* del settore, ha fornito concreti suggerimenti quali l'utilizzo di sistemi di crittografia, lo svolgimento di test preventivi di sicurezza, l'implementazione di procedure di monitoraggio degli accessi non autorizzati, la minimizzazione dei dati, la formazione del personale, il rafforzamento dei meccanismi di autenticazione, l'adozione di sistemi sicuri di cancellazione dei dati (cc.dd. *secured dumpsters*), nonché il monitoraggio del livello di *data security* e *data privacy* assicurato dalle terze parti coinvolte nel processo di trattamento dei dati[793].

Al di dà dello specifico caso della violazione di "promesse" compiute per il tramite delle *proprie privacy policies*, la FTC ha progressivamente esteso la nozione di

[791] *FTC v. CompuCredit Corporation e Jefferson Capital Systems, LLC*. Civil No. 1:08-CV-1976-BBM-RGV 2008. Cfr. *Big Data: A Tool for Inclusion or Exclusion?* (FEDERAL TRADE COMMISSION, 2016), 22; G. BODEA, K. KARANIKOLOVA, D.K. MULLIGAN, J. MAKAGON, *Automated decision-making on the basis of personal data that has been transferred from the EU to companies certified under the EU-U.S. Privacy Shield Fact-finding and assessment of safeguards provided by U.S. law* (COMMISSIONE EUROPEA, 2018), 95.

[792] Per riflessioni generali sul significato della nozione di "reasonable security" si veda T.J. SMEDINGHOFF, *Defining the Legal Standard for Information Security: What Does "Reasonable" Security Really Mean?*, in A. CHANDER, L. GELMAN, M.J. RADIN (a cura di), *Securing Privacy in the Internet Age*, Standford University Press, Standford, 2008, 19ss.

[793] J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 6ss. *Ex multis*, *In re Petco Animal Supplies, Inc*., 139 F.T.C. 102, 104-05 (2005); *In re Guess?, Inc*., 136 F.T.C. 507, 510-11 (2003); Cbr Sys., Inc., FTC File No. 112 3120, No. C-4400 (F.T.C. Apr. 29, 2013); *In re Lookout Servs., Inc*., 151 F.T.C. 532, 535 (2011); *In re EPN, Inc.*, FTC File No. 112 3143, No. C-4370 (F.T.C. June 7, 2012); In re Nationwide Mortg. Grp., Inc., 139 F.T.C. 245, 247-48 (2005); *In re ACRAnet, Inc*., FTC File No. 092 3088, No. C-4331 (F.T.C. Aug. 17, 2011). Per una più ampia casistica si veda D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., spec. ntt. 331-351.

deception a qualsiasi condotta ingannevole che, a prescindere dal contenuto e dall'esistenza di *privacy policies*, si traduca in un accesso non autorizzato ai dati personali[794]. Più specificatamente, la Commissione ha teorizzato due tipologie di *general deception*: la "*false affiliation*" e il "*false claim of need to provide information*" tipicamente rinvenibili in ipotesi di frodi di *phishing* (specialmente nel caso di *man-in-the-browser*)[795] e di *pretexting*[796].

Infine, fra le ipotesi di pratiche commerciali sanzionate in quanto "ingannevoli" dalla FTC rientrano anche le fattispecie di "*insufficient notice*" integrate, ad esempio, da cambiamenti delle privacy policies non preventivamente notificati alla clientela[797], ovvero da *privacy policies*, termini e condizioni del servizio, contratti di licenza d'uso di

[794] Nel caso *FTC v. ReverseAuction.com*, ad esempio, la FTC sanzionò la pratica con cui la *ReverseAuction*, inviando messaggi di posta elettronica segnalanti false scadenze dei propri user ID, induceva gli utenti di eBay a comunicargli i propri dati di autenticazione. *FTC v. ReverseAuction.com*, No. 00-CV-00032 (D.D.C. Jan. 6, 2000). Analoghe le accuse avanzate in *FTC v. Sun Spectrum Commc'ns Org., Inc*., No. 03-CV-8110 (S.D. Fla. Oct. 3, 2005).

[795] Sulla differenza tra le due fattispecie si veda la copiosa giurisprudenza dell'Arbitro Bancario Finanziario, *ex multis*, Collegio di Coordinamento, Decisione N. 3498 del 26 ottobre 2012 in cui venne precisato come "[a] differenza che nelle fattispecie "classiche" sin qui note, dove l'aggiramento dei presidi di sicurezza e la circonvenzione del cliente ha luogo attraverso metodi ormai noti (email civetta, false comunicazioni di scadenza, invito all'aggiornamento di database e così via) […] [i]l principio operativo [del] man-in-the-browser [prevede la generazione di] quella che in gergo suole definirsi una botnet, ossia per l'appunto una rete di macchine egualmente infettate dallo stesso virus. Il malware – riconducibile alla più ampia categoria dei cc.dd. trojan ("cavalli di Troia") e dotato di sofisticate capacità di elusione dei migliori antivirus – si annida in modo silenzioso nel computer della vittima senza creare alcun malfunzionamento o alterazione del sistema tali da attrarre l'attenzione dell'utente. Il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli che il programma abbia posto nel mirino (*targeted banks*). In quel preciso istante il *malware* "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quella originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, *Hyper Text Transfer Protocol*) "http" e non già "https" (dove la "s" finale sta per *secured*, protetto)." Cfr. R. MANENTI e G. MARZIALE, *Delle obbligazioni*, in S. RUPERTO (con il coordinamento di), *La giurisprudenza sul codice civile coordinata con la dottrina*. *Libro IV delle obbligazioni (artt. 1823-1935)*, Milano, Giuffrè, 2012, 368 ss; *FTC v. Hill*, No. 03-5537 (S.D. Tex. Mar. 22, 2004), 10-11.

[796] Secondo la definizione elaborata dalla FTC tale pratica consiste in "*making various misleading and false statements to financial institutions and others. Such tactics include calling financial institutions and pretending to be the account holder, thereby inducing the financial institution to disclose private financial information*" che poi vengono vendute. Così *FTC v. Rapp*, No. 99-WM-783 (D. Colo. Apr. 21, 1999) citato da D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 633; A.C. RAUL, C.C. FRONZONE e S.S. TAPIA, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 401ss.

[797] E.g. *In re Facebook, Inc*., FTC File No. 092 3184, No. C-4365 (F.T.C. July 27, 2012).

software o qualsiasi altra comunicazione fornita alla clientela recanti descrizioni delle modalità di trattamenti dei dati personali intenzionalmente omissive o ambigue[798].

Più limitate, invece, le teorizzazioni sviluppate dalla FTC con riferimento alla nozione di "*unfairness*", generalmente associata a condotte che hanno causato o sono astrattamente idonee a causare una "*substantial injury*" non ragionevolmente evitabile dai consumatori e non controbilanciata da preponderanti benefici per i consumatori stessi ovvero per la concorrenza (c.d. *three-part test*)[799]. In tal senso, la FTC ha qualificato come "*unfair*" pratiche commerciali ritenute lesive dell'autodeterminazione dei consumatori poiché volte a creare o sfruttare ostacoli al libro sviluppo dei processi decisionali della clientela[800]. In materia di *data privacy*, tali presupposti potrebbero essere integrati da cambiamenti retroattivi delle *privacy policies*, raccolte ingannevoli di dati personali, utilizzi impropri di dei dati raccolti, ovvero dall'implementazione di "*deceitful or obstructionist default settings*" come, ad esempio, nel caso in cui la disinstallazione di un software risulti poco intuitiva e provochi ingiustificati successivi malfunzionamenti di altre componenti software e hardware del dispositivo[801].

3.8.1. La potestà legislativa della FTC: il futuro della data privacy statunitense?

Ai sensi della sezione 18 del *FTC Act* la potestà normativa della FTC si distingue in non legislativa e legislativa. La prima consiste nella formulazione di "*interpretive rules and general statements of policy with respect to unfair or deceptive acts or practices*"[802], mentre la seconda è definita come il potere di adottare "*rules which define with specificity*

[798] Come chiaramente spiegato in dottrina "[*t*]*he FTC has thus indicated it will reject as inadequate notices that are technically correct yet not sufficiently complete in explaining a company's practices*." D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 659. È questo, ad esempio, quanto rilevato dalla FTC in *In re Sears Holdings Mgmt. Corp*., FTC File No. 082 3099, No. C-4264 (F.T.C. Aug. 31, 2009) e *FTC v. Frostwire*, LLC, No. 1:11-cv-23643 (S.D. Fla. Oct. 12, 2011).

[799] 15 U.S.C. § 45(n).

[800] *In re Int'l Harvester Co*., 104 F.T.C. 949 app. at 1070-76 (1984).

[801] Questo è quanto avvenuto in *In re Sony BMG Music Entm't*, FTC File No. 062 3019, No. C-4195 (F.T.C. June 28, 2007). Cfr. D.J. SOLOVE e W. HARTZOG, The FTC and the New Common Law of Privacy, cit., 640.

[802] 15 USCA § 57a (a)(1)(A). Cfr. G.M. STEGMAIER, W. BARTNICK, Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine, 5, *J. Internet L*., 2013, 17ss.

acts or practices which are unfair or deceptive acts or practices in or affecting commerce" (c.d. *Magnuson-Moss rulemaking*)[803].

Come fin qui illustrato, nell'esercitare i suoi poteri in materia di *data privacy* e *security* la FTC ha prediletto lo strumento della *non-legislative guidance*, non soltanto attraverso la menzionata prassi dei *consent orders* di matrice stragiudiziale e casistica, ma anche attraverso l'adozione di più generiche linee guida[804]. Se tale approccio si giustificava per la natura embrionale del contesto digitale e, conseguentemente, della necessità di mantenere un quadro normativo flessibile idoneo a adattarsi alle rapide evoluzioni del mercato *data-driven*[805], iniziano ad emergere dubbi sulla perdurante adeguatezza del modello al contesto attuale. In particolare, si è fatto innanzitutto notare come la tendenziale uniformità dei *consent orders* abbia, da un lato, dimostrato la capacità della FTC di dettare regole di condotta idonee a sopravvivere ai cambiamenti tecnologici e, dall'altro, favorito la sedimentazione delle stesse tra i soggetti vigilati, assurgendo *de facto* a regole di condotta per gli stessi[806].

D'altro canto, il carattere casistico e non generalmente vincolante dei *consent orders*, associato alle resistenze mostrate dal Congresso verso l'introduzione di una legislazione federale trans-settoriale in materia di *data privacy*, ha stimolato una riconsiderazione dell'opportunità di sfruttare le potestà legislative attribuite alla FTC per colmare tale vuoto normativo. La potestà di *Magnuson-Moss rulemaking*, infatti, rappresenterebbe un buon compromesso in quanto più complessa e garantista del mero

[803] 15 USCA § 57a (a)(1)(B).

[804] Per considerazioni sulla meritevolezza del peso interpretative esercitato dagli orientamenti della FTC sulle determinazioni giurisprudenziali in quanto "quasi-precedente" si veda *Skidmore v. Swift & Co*., 65 S. Ct. 161, 164 (1944) nonché quanto statuito in 5 U.S.C. § 552(a)(2) (2012). Cfr. *Privacy & Data Security Update (2017): An Overview Of The Commission's Enforcement, Policy Initiatives, And Consumer Outreach And Business Guidance In The Areas Of Privacy And Data Security*, (FEDERAL TRADE COMMISSION, 2017); *Protecting Personal Information: A Guide For Business* (FEDERAL TRADE COMMISSION, 2016).

[805] Sul rischio di rapida obsoloscenza di interventi legislativi si veda *FTC v. Wyndham Worldwide Corp*., No. 2:12-cv-01365-PHX-PGR (D. Ariz. Aug. 9, 2012), 7 nella parte in cui, citando *Chenery Corp*., 67 S. Ct. 1580, viene ribadito come "[*d*]*ata security industry standards are continually changing in response to evolving threats and new vulnerabilities and, as such, are 'so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule*." Cfr. R.A. ANTHONY, Interpretive Rules, Policy Statements, Guidances, Manuals, and the Like—Should Federal Agencies Use Them to Bind the Public?, 41 *Duke L. J*., 1992, 1311, 1325; J.W. BINKLEY, Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement After Wyndham, 31, *Berkeley Tech. L.J.*, 2016, 1079ss.

[806] Cfr. G.M. STEGMAIER, W. BARTNICK, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements, 20 *Geo. Mason L. Rev*., 2013, 673, 713.

notice-and-comment amministrativo, ma più flessibile dell'ordinaria attività parlamentare (si parla, infatti, di "*hybrid rulemaking*")[807].

In particolare, ai sensi del *Magnuson-Moss Warranty–Federal Trade Commission Improvement Act*[808] tale procedura para-legislativa prevede una partecipazione pubblica rafforzata[809] attraverso: (i) la pubblicazione della regolamentazione proposta in pubblica consultazione[810]; (ii) la pubblicazione di tutte le informazioni, opinioni e osservazioni pervenute[811]; (iii) la possibilità per le parti interessate di intervenire in audizioni informali[812] presiedute da un *hearing officer* indipendente deputato a formulare proposte di decisioni basate sulle risultanze dell'audizione[813].

Come accennato, la FTC tende ad evitare il ricorso all'autorità di *Magnuson-Moss rulemaking* poiché ritenuta proceduralmente eccessiva rispetto alla verosimile rapida obsolescenza della disciplina del settore *data-driven*[814]. Tale scelta, tuttavia, è stata recentemente messa in discussione non soltanto dalla dottrina, ma anche dalla giurisprudenza nel recente caso LabMD, in un tale laboratorio analisi privato è stato accusato di aver posto in essere "*unfair data security practices*" sfociate poi in un massiccio accesso non autorizzato a dati sanitari particolarmente sensibili della propria clientela, resi pubblicamente accessibili online[815].

La particolarità del caso risiede innanzitutto nella scelta di LabMD di rifiutare la conclusione transattiva del procedimento e sottoporre il provvedimento della FTC al vaglio del giudice amministrativo che ritenne non adeguatamente provata l'idoneità della condotta censurata a provocare la "*substantial consumer injury*" di cui alla sezione 5(n)

---

[807] Così P. STRAUSS, T. RAKOFF, C. FARINA e G. METZGER, *Gellhorn and Byse's Administrative Law: Cases and Comments*, XI ed., Foundation Press, 2011, 129. Cfr. T. GARVEY, *A Brief Overview of Rulemaking and Judicial Review* (CONGRESSIONAL RESEARCH SERVICE, 2017), 4.

[808] 15 U.S.C. §§ 45–46, 49–52, 56– 57c, 2301–2312 (2012).

[809] Cfr. W. FUNK, Public Participation and Transparency in Administrative Law – Three Examples as an Object Lesson, 61, *Admin. L. Rev.*, 2009, 171, 172–77.

[810] 15 USCA § 57a (b) (1) (A).

[811] 15 USCA § 57a (b) (1) (B).

[812] In particolare, la normativa prevede la facoltà degli interessati di presentare le proprie posizioni oralmente o per iscritto e, ove la Commissione lo ritenga necessario al fine di chiarire divergenti rappresentazioni fattuali, di presentare cc.dd. *rebuttal submissions*, ovvero di condurre *cross-examinations* ove la FTC le ritenga adeguate e necessarie ad una piena e veritiera rappresentazione delle circostanze alla base del problema15 USCA § 57a (b) (1) (A), (B) e (C).

[813] 15 USCA § 57a (c) (1) (B)

[814] In questo senso, ad esempio, si è espresso J.S. LUBBERS, It's Time to Remove the "Mossified" Procedures for FTC Rulemaking, 83, *Geo. Wash. L. Rev.*, 2015, 1979ss.

[815] *LabMD, Inc*., FTC File No. 102-3099, No. C-9357, 9 (F.T.C. July 29, 2016). Cfr. J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 10ss.

FTC Act. Secondo la Corte, infatti, la mera "possibilità" del verificarsi del danno, provata dalla FTC, non sarebbe di per sé sufficiente ad integrare il carattere "sostanziale" dell'ipotetico pregiudizio, essendo necessaria anche la prova della "probabilità" del verificarsi dell'evento dannoso[816]. I tre commissari della FTC rifiutarono la posizione assunta dal giudice ed emisero un *final order* verso LabMD chiarendo come la particolare gravità del pregiudizio a cui gli utenti del laboratorio erano stati astrattamente esposti avesse reso sufficiente una più attenuata valutazione probabilistica del verificarsi dello stesso[817]. Inoltre, quanto al carattere "sostanziale" del danno subito, la FTC precisò che anche danni reputazionali ed emotivi risultano "*real and substantial and thus cognizable under Section 5(n)*[818]*."*

Tale approccio flessibile e di evidente *favor* per i consumatori è stato particolarmente apprezzato in dottrina[819]. Ciò in quanto, come recentemente ribadito nel caso Spokeo[820], il carattere difficilmente quantificabile e (generalmente) meramente

[816] *Initial Decision, LabMD, Inc*., FTC File No. 102-3099, No. C-9357, 92 (F.T.C. Nov. 12, 2015). Cfr. K. PHAN, T. FLO, R. PATEL, Recent Trends in the FTC's Data Security and Privacy Enforcement Actions, 19, *J. Internet L*., 2016, 17ss.

[817] Cfr. *LabMD, Inc*., FTC File No. 102-3099, No. C-9357, 10 e 21 in cui viene chiarito come "*in extreme cases, subjective types of harm might well be considered as the basis for a finding of unfairness* […] *a practice may be unfair if the magnitude of the potential injury is large, even if the likelihood of the injury occurring is low*.".

[818] 15 U.S.C. § 45(n) (2012); *LabMD, Inc.*, FTC File No. 102-3099, No. C-9357 (F.T.C. July 28, 2016) (Final Order).

[819] I. DAVIS, Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads, Emory Law Journal (Forthcoming), 2019, disponibile su *ssrn.com*.

[820] Il caso prese le mosse dall'azione intentata dal Sig. Thomas Robins contro Spokeo, Inc., gestore di un "*people search engine*" che aggrega dati personali di individui al fine di condividerli con i propri utenti quali, ad esempio, datori di lavoro in cerca di personale. Avendo scoperto che il suo profilo Spokeo gli attribuiva una formazione e posizione lavorativa migliore di quella reale, il Sig. Robins divenne promotore di un'azione di classe lamentando la violazione del FCRA da parte di Spokeo Inc., accusato di aver omesso di implementare misure adeguate ad assicurare la veridicità delle informazioni disseminate per il tramite della propria piattaforma. La corte distrettuale, tuttavia, rigettò la domanda attorea ritenendo che la difficoltà a trovare impiego e lo stress conseguitone non fossero idonei a configurare un concreto interesse ad agire (*Robins v. Spokeo, Inc*., No. CV10–05306, 2011 WL 597867 1–2). Il *Ninth Circuit*, al contrario, ritenne che la violazione di diritti riconosciuti da espressa previsione legislativa fosse, di norma, sufficiente ad attribuire legittimazione attiva, specialmente ove, come avvenuto nel caso di specie, l'attore lamenti la violazione di diritti individuali e non soltanto collettivi (*Robins v. Spokeo, Inc*., 742 F.3d 9th Cir. 2014). La Corte Suprema, investita della questione, rinviò nuovamente la decisione al *Ninth Circuit* ritenendo non adeguatamente motivato il carattere concreto e attuale del danno lamentato che, per quanto intangibile, non può essere meramente astratto e procedurale (*Spokeo, Inc. v. Robins*, 136 S. 2016). Nel pronunciarsi sul rinvio, la Corte si avvalse del "test di concretezza" sviluppato dal *Second Circuit* nel caso *Strubel v. Comenity Bank*, consistente nel verificare se, da un lato, la previsione legislativa violata miri a proteggere un interesse sostanziale e non meramente procedurale e, dall'altro, se la specifica violazione allegata dall'attore sia sfociata in un effettivo danno o presenti un significativo rischio di danno. In quest'ottica, il giudice O'Scannlain ritenne che, sotto il primo profilo, il carattere ubiquitario dei *credit reports* rende evidente la natura sostanziale dell'interesse che la norma intende proteggere nel prevenire la trasmissione di informazioni non veritiere a futuri potenziali datori di lavoro. Dal punto di vista della concretezza del danno, invece, il giudice chiarì che, sebbene non ogni violazione di obblighi procedurali possa sfociare in un danno risarcibile, "*even seemingly flattering inaccuracies can hurt an individual's*

potenziale dei pregiudizi derivanti da *data breaches* rende particolarmente ardua la prova del carattere "attuale" o "imminente" del danno imposto dall'articolo III della *standing doctrine*[821], con conseguente frequente improcedibilità dell'azione davanti alle corti federali[822].

Tale apprezzamento non è stato condiviso da LabMD che, appellato il *final order*, oltre ad insistere sul carattere meramente potenziale dei danni lamentati dagli attori, contestò l'eccessiva vaghezza dell'ordine con il quale la FTC oltre ad imporre la predisposizione di una valutazione d'impatto e la designazione di un dipendente responsabile della supervisione del programma di *data security*, aveva richiesto la l'implementazione di misure di sicurezza adeguate al controllo e alla prevenzione dei rischi rilevati per mezzo della summenzionata valutazione. Interventi correttivi, questi, accompagnati dall'obbligo di sottoporsi a periodiche revisioni da parte di un ispettore esterno per un periodo stimato di venti anni[823].

L'*Eleven Circuit*, investito della questione, rigettò il primo motivo di appello, sostanzialmente avallando la valutazione della FTC circa il carattere illegittimo e negligente della condotta del laboratorio e, quindi, del carattere sostanziale del danno prodotto seppure soltanto a livello potenziale, ma accolse il secondo. A tale ultimo riguardo la Corte, rilevando la mancanza di indicazioni sufficientemente specifiche sulle

employment prospects as they may cause a prospective employer to question the applicant's truthfulness or to determine that he is overqualified." Nel caso *re Horizon Healthcare Servs. Inc. Data Breach Litig*. (846 F.3d Cir. 2017), invece, la Corte si è avvalsa di un diverso test di concretezza fondato sul concetto di "*material risk of harm*". In ultima analisi, la giurisprudenza sembrerebbe essersi premurata di preservare gli incentivi individuali alla contestazione giurisdizionale di danni riconducibili a illegittimi trattamenti di dati imputabili ai grandi operatori della rete, per quanto di difficile quantificazione. Cfr. R.H. FALLON, Jr., The Linkage Between Justiciability and Remedies — And Their Connections to Substantive Rights, 92 *Va. L. Rev*. 633, 637 (2006); T. KASPEREK SOMES, Assessing Spokeo, Inc. v. Robins: The Future of Statutory Damage Class Actions in the Consumer Protection Arena, 20, *J. Consumer & Com. L*., 2017, 122, 124; D. TOWNSEND, Who Should Define Injuries for Article III Standing?, 68, *Stan. L. Rev. Online*, 2015, 76, 80; Robins v. Spokeo, Inc.: Ninth Circuit Allows Fair Credit Reporting Act Class Action to Proceed Past Standing Challenge 131 *Harv. L. Rev*., 2018, 894 ss.

[821] 28 U.S.C. § 1332(a)(1) (2012).

[822] Cfr. D.J. SOLOVE, D. KEATS CITRON, Risk and Anxiety: A Theory of Data-Breach Harms, 96, *Tex. L. Rev*., 2018, 737, 745 ss.

[823] *LabMD, Inc*., FTC File No. 102-3099, No. C-9357, at 2–3 (F.T.C. July 28, 2016) (Final Order). Per riflessioni sugli affini poteri investigative attribuiti alle Autorità nazionali competenti in materia di vigilanza sulla disciplina della protezione dei dati personali, e il loro ruolo nello sciogliere molti nodi intorno al concetto di trasparenza e spiegazione dei processi decisionali automatizzati si veda B. Casey, A. Farhangi, R. Vogl, Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise, cit., 143 ss.

modalità pratiche di implementazione misure correttive, definì l'ordine della Commissione un "*indeterminable standard of reasonableness"*[824].

In attesa di conoscere la reazione della FTC, le conclusioni raggiunte dalla Corte, se lette alla luce della più volte menzionata uniformità del contenuto degli ordini nel tempo emessi dalla Commissione, lasciano prevedere una sensibile riduzione della predisposizione degli operatori del settore ad accettare generici *consent orders*. Ne deriva un'esigenza di ripensamento delle prassi di vigilanza finora predilette dalla Commissione non soltanto in chiave più dettagliata, ma anche vincolante, rendendo così l'esercizio della autorità di *Magnuson-Moss rulemaking* la soluzione più idonea a tradurre l'esperienza stragiudiziale finora maturata in una serie di puntuali regole di condotta[825].

D'altro canto, anche le obiezioni di chi riteneva la complessità procedimentale della *Magnuson-Moss rulemaking* sproporzionata agli interessi sottesi alla disciplina sulla *data privacy* sono state progressivamente superate per effetto della proliferazione delle pratiche commerciali aventi ad oggetto il trattamento dei dati personali della clientela, dell'aggravarsi dei rischi connessi all'utilizzo di tecnologie sempre più invasive, nonché dell'accresciuta domanda di chiarezza proveniente dagli operatori del settore[826].

L'esercizio di tale potestà legislativa della FTC, peraltro, apporterebbe benefici anche sul versante dell'efficientamento dell'azione amministrativa. In primo luogo, il coinvolgimento dei soggetti vigilati consentito dal regime di partecipazione pubblica imposto dalla procedura *Magnuson-Moss rulemaking* contribuirebbe a migliorare la qualità degli orientamenti assunti dalla FTC[827]. In secondo luogo, l'introduzione di un quadro normativo vincolante contribuirebbe a ridurre, nel lungo termine, i costi di

[824] *LabMD, Inc*., 894 F.3d, 1236 come citato da I. DAVIS, Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads, Emory Law Journal (Forthcoming), 2019, disponibile su *ssrn.com.* Cfr. S. SARGENT, Fight or Comply: the Federal Trade Commission's Power to Hold Companies Liable for Data Security Breaches, 41, *J. Corp. L*., 2015, 529ss.

[825] I. DAVIS, Resurrecting Magnuson-Moss Rulemaking: The FTC at a Data Security Crossroads, Emory Law Journal (Forthcoming), 2019, disponibile su *ssrn.com.*

[826] C.J. SPINELLI, Far From Fair, Farther From Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking, 6, *Am. Univ. Leg. And Policy Brief*, 2014, 129, 134; W. HARTZOG, D.J. SOLOVE, The Scope and Potential of FTC Data Protection, 83, *Geo. Wash. L. Rev*., 2015, 2230, 2258; J.S. LUBBERS, It's Time to Remove the 'Mossified' Procedures for Removing FTC Rulemaking, 83, *Geo. Wash. L. Rev*. 2015, 1979, 1997-8; C.H. KOCH JR.. B. MARTIN, FTC Rulemaking through Negotiation, 61, *N.C. L. Rev*., 1983, 275, 290.

[827] Cfr. R.J. PIERCE, Two Problems in Administrative Law: Political Polarity on the District of Columbia Circuit and Judicial Deterrence of Agency Rulemaking, *Duke L. J*., 1988, 300, 308–09; G.M. STEGMAIER, W. BARTNICK, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements, 20, *Geo. Mason L. Rev*., 2013, 673, 710.

enforcement moltiplicati dalla tendenza all'impugnazione dei *consent orders* verosimilmente inaugurata dalla giurisprudenza LabMD[828]. Infine, l'esercizio della sua potestà legislativa consentirebbe alla FTC di rafforzare la tutela dei consumatori avendo legittimazione attiva diretta per adire la corte federale in ogni caso di violazione delle regole di condotta così fissate, senza dover attendere una eventuale seconda violazione delle misure imposte nel *consent order*[829].

3.9. Verso una *data privacy* trans-settoriale: il *California Consumer Privacy Protection Act* e gli *ALI Data Privacy Principles*

La ricostruzione sin qui condotta dei frammenti legislativi e giurisprudenziali che vanno a comporre il mosaico normativo statunitense in materia di protezione dei dati personali, come più volte ribadito, mostra, allo stato dell'arte, delle lacune troppo spesso incolmabili dall'interprete. In particolare, il carattere settoriale e limitato dell'ambito di applicazione del FCRA e dell'ECOA, così come dei poteri di vigilanza della FTC, nonché l'esclusiva attenzione prestata alle esigenze di tutela della riservatezza avverso interferenze di enti pubblici sfociata nella copiosa giurisprudenza sul Quarto emendamento, nella puntuale disciplina dell'ECPA e della *Due Process Clause* finiscono per rendere "*the surreptitious collection of private information regarding web surfing habits, or consumer purchases*, […] *generally legal*[830]*."*

Ciononostante, la crescita esponenziale del peso economico del mercato dei dati, anche e soprattutto transfrontaliero, ha posto l'accento sull'esigenza di ricercare un compromesso legislativo idoneo a ridurre il divario sempre più profondo nel livello di protezione dei dati garantito nell'Unione europea e negli Stati Uniti[831]. Tuttavia, al di là della dubbia "equivalenza" del regime informativo dettato in punto di processi decisionali

[828] P. STRAUSS, T. RAKOFF, C. FARINA e G. METZGER, *Gellhorn and Byse's Administrative Law: Cases and Comments*, XI ed., Foundation Press, 2011, 420; S.L. PARDAU, B. EDWARDS, The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity, 12, *J. Of Bus. & Tech. L.*, 2017, 227, 242; C.S. DIVER, The Optimal Precision of Administrative Rules, 93 *Yale L. J.*, 1983, 65, 73.

[829] Cfr. M. MINZNER, Why Agencies Punish, 53 *Wm. & Mary L. Rev.*, 2012, 853, 856; G.M. STEGMAIER, W. BARTNICK, Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements, 20, *Geo. Mason L. Rev.*, 2013, 673, 712.

[830] R.J. KROTOSZYNSKI JR, *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford, Oxford University Press, 2016, 17-18.

[831] Confermato dalla recente invalidazione dello Scudo UE-USA per la privacy. Su tale vicenda si veda meglio quando detto *supra sub* par. 3.1.

automatizzati, rispetto al quale però, come già visto, la Commissione aveva previsto un mero monitoraggio dell'incidenza del fenomeno sul traffico transfrontaliero dei dati provenienti dall'Unione europea, ritenuta, allo stato attuale, troppo limitata da imporre il rispetto di specifici standard paneuropei, le rinnovate esigenze di adeguatezza delle tutele apprestate negli USA al trattamento dei dati personali, hanno stimolato un rinvigorito attivismo legislativo[832].

In questo senso, abbandonata la prospettiva sin qui assunta per mettere in luce i limiti che l'attuale conformazione dell'ordinamento statunitense mostra nel contesto digitale in generale, e in quello dei processi decisionali automatizzati in particolare, si conclude il capitolo assumendo un'ottica prospettica. Più specificamente, si tenterà di tracciare le embrionali linee evolutive emergenti dal raffronto della direzione normativa assunta nei due più recenti passi compiuti verso l'adozione di una legislazione federale trans-settoriale in materia di *data privacy*: il *California Consumer Privacy Act* e i *Data Privacy Principles* dell'*American Law Institute*.

Entrato in vigore il 1° gennaio 2020, il *California Consumer Privacy Act* (CCPA)[833] rappresenta il primo tentativo, seppure a livello squisitamente statale[834], di

[832] Scudo UE-USA per la privacy, § 25.

[833] CAL. CIV. CODE §§ 1798.100-.192 (West 2018). Cfr. A.C. RAUL, C.C. FRONZONE e S.S. TAPIA, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 416ss.

[834] Allo stato attuale risultano essere state avanzate proposte legislative in materia di *data privacy* in almeno 25 Stati. Molti di questi tentativi sono risultati infruttuosi, tuttavia, sono pur sempre sintomo di una rinnovata attenzione al tema. In Connecticut, ad esempio, è stata creata un *Task Force* al fine di condurre un'indagine volta ad individuare quali categorie di dati i titolari del trattamento dovrebbero essere tenuti a condividere con gli interessati. Lo stesso è avvenuto nelle Hawaii dove, tuttavia, il Governatore ha posto il veto sulla proposta di introduzione di un divieto di vendita dei dati di geolocalizzazione degli interessati in mancanza del previo consenso esplicito degli stessi. In Illinois il *Genetic Information Privacy Act* è stato emendato al fine di impedire la trasmissione di dati sanitari raccolti da laboratori privati a compagnie assicurative. In Lousiana è stata istituita una *Task Force* deputata ad investigare gli effetti della vendita di dati personali degli utenti da parte di ISPs ed è stato disposto il divieto per i *provider of broadband Internet access service* di raccogliere, vendere, o in altro modo trattare dati personali degli utenti in mancanza di previo consenso ovvero di una delle altre basi giuridiche individuate. In Mississippi, invece, il tentativo di introdurre un corpo normativo analogo al CCPA (denominato *Mississippi Consumer Privacy Act*) è fallito. Analoga la sorte del *Montana Biometric Information Privacy Act*. In molti altri Stati (quali New Jersey, Rhode Island, South Carolina, Pennsylvania e Washington), incluso quello di New York, sono pendenti numerose iniziative legislative volte ad aggiornare la disciplina vigente, così come ad introdurre nuovi corpi legislativi. Emblematica, in questo senso, la proposta avanzata nello Stato di New York di introduzione del c.d. "*It's Your Data Act*" volto a dettare un generale regime di tutela in materia di protezione dei dati personali. Per maggiori dettagli sulle varie iniziative avviate a livello statale negli Stati Uniti si veda quanto riportato nella pagina web curata dalla NATIONAL CONFERENCE OF STATE LEGISLATURES, *2019 Consumer Data Privacy Legislation* disponibile all'indirizzo *www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.*
Per una generale ricognizione della portata normativa del CCPA si veda W.C. FREEMAN, *California Dreamin' of Privacy Regulation: The California Consumer Privacy Act and Congress* (CONGRESSIONAL

introduzione oltreoceano di una disciplina genericamente volta a disciplinare la "raccolta"[835] di dati personali a "fini commerciali"[836]. Dal canto loro, invece, i *Data Privacy Principles* sono il prodotto di un'iniziativa avviata oltre sette anni fa dall'ALI e volta a formulare dei "*twenty-first century concepts of privacy law*" che, come già avvenuto negli anni '70 per la codificazione dei menzionati *Privacy Torts* di cui al *Restatement* (*Second*) *of Torts*, potessero, nel lungo termine, guidare legislatori, agenzie amministrative e attori privati verso una nuova *U.S. data privacy law*[837] e che, nel breve periodo, riuscissero a rivitalizzare il ruolo dei *Fair Information Practice Principles* (FIPPs)[838].

Passando all'analisi dell'ambito materiale di applicazione, ed iniziando dalla tecnica definitoria prescelta, se l'ALI ha prediletto l'adozione della terminologia del GDPR specialmente con riguardo alle nozioni base di titolare e responsabile del

---

RESEARCH SERVICE, novembre 2018); W. HARTZOG, N. RICHARDS, Privacy's Constitutional Moment and the Limits of Data Protection, 61, *Boston College Law Review*, 2020, 1687ss.

[835] Per "raccolta" di dati personali si intende l'acquisto, l'affitto, l'aggregazione, la ricezione ovvero l'accesso con qualsiasi altro mezzo a dati personali dei consumatori. CAL. CIV. CODE §§ 1798.140 (e). A ulteriore chiarimento, è interessante notare come il legislatore californiano abbia puntualizzato che non si può parlare di "vendita" di dati personali quando l'imprenditore trasferisce il proprio patrimonio informativo a un soggetto terzo come asset in una fusione, acquisizione, procedura fallimentare o qualsiasi altra transizione in un cui tale soggetto terzo assume il controllo di tutto o parte dell'assetto imprenditoriale dell'originario titolare del trattamento. Unico limite è che in questi casi, ove il soggetto terzo intenda utilizzare tali informazioni per finalità "materialmente" incompatibili con le dichiarazioni precedentemente rilasciate dal titolare del trattamento acquisito, è necessario notificare tali mutamenti alla clientela non essendo per tal via autorizzate modifiche retroattive alle privacy *policies*. CAL. CIV. CODE §§ 1798.140 (D).

[836] Per finalità commerciali si intende il perseguimento di interessi commerciali o economici quali l'induzione di un'altra persona a compiere acquisti, a sottoscrivere abbonamenti, a scambiare beni, informazioni o servizi, ovvero a compiere, direttamente o indirettamente, una transazione commerciale. Sono invece espressamente escluse finalità di manifestazione di pensiero "non commerciale" quale quello di natura politica o giornalistica. CAL. CIV. CODE §§ 1798.140 (f).

[837] D.J. SOLOVE, P.M. SCHWARTZ, ALI Data Privacy: Overview and Black Letter Text, 68, *UCLA Law Review*, 2020 disponibile su *ssrn.com*.

[838] I FIPPs, sono stati inizialmente elaborati dallo *U.S. Department of Health, Education, and Welfare* (HEW) nel 1973 e poi più volte ripresi e rivisitati, specialmente nel 1980 da parte dell'*Organization for Economic Co-operation and Development* (OECD) (aggiornati nel 2013). Questa versione, infatti, rappresenta l'esempio più completo e utilizzato di linee guida in materia di *data privacy*, punto di riferimento anche in fase di sviluppo della Direttiva Madre. Si tratta di una serie di principi cardine che negli Stati Uniti si sono progressivamente tradotti nel noto approccio di "*notice-and-consent*". Tipicamente, tale regime si è declinato nella predisposizione di *privacy policies* rispetto alle quali gli interessati possono esercitare facoltà di scelta, prima fra tutte quella di *opt-out*. Il carattere notoriamente illusorio del "consenso" in tal modo raccolto, tuttavia, ne ha decretato il sostanziale fallimento. *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2013). Cfr. C.J. HOOFNAGLE, *Federal Trade Commission Privacy Law And Policy*, Cambridge University Press, Cambridge, 2016, 365; P.M. SCHWARTZ, Internet Privacy and the State, cit., 821-23; O. BEN-SHAHAR, C. SCHNEIDER, *More Than You Want To Know: The Failure Of Mandated Consent*, Princeton University Press, Princeton, 2014, 55ss; W. HARTZOG, The Inadequate, Invaluable Fair Information Practices, 76 *Md. L. Rev*., 2017, 952; D.J. SOLOVE, Privacy Self-Management and the Consent Dilemma, 126, *Harv. L. Rev*., 2013, 1880, 1886.

trattamento[839], il CCPA ha optato per la convergenza di entrambi i ruoli nella diversa figura del "*business*"[840] caratterizzato cumulativamente: (i) dallo svolgimento di attività di raccolta di informazioni personali nel proprio interesse; (ii) dalla determinazione (in via autonoma o in coordinamento con altri) delle finalità e dei mezzi del trattamento dei dati; (iii) dall'esercizio della propria attività nello Stato della California; e, alternativamente (iv) dal conseguimento di un profitto lordo superiore ai venticinque milioni di dollari; (iv-*bis*) dall'acquisto/ricezione/vendita/condivisione, su base annuale, dati personali di oltre cinquantamila consumatori per finalità commerciali; ovvero (iv-*ter*) dalla provenienza di almeno il 50% del proprio profitto annuale dalla vendita di dati personali[841].

Particolarmente problematico, inoltre, si è rivelato il tentativo di armonizzazione della nozione di dato personale il quale, pur noto e utilizzato dal legislatore statunitense[842], ha assunto accezioni non sempre uniformi e spesso tese ad escludere informazioni che il legislatore eurounitario definisce come "riferibil[i] ad una persona fisica […] identificabile[843]". Le cc.dd. "*personally identifiable information*" (cc.dd. PPI), infatti, sono state soltanto più recentemente oggetto di attenzione normativa negli Stati Uniti[844]. In particolare, nonostante il CCPA le abbia assimilate alle "*personal information*[845]*"* e la FTC abbia riconosciuto la necessità di prendere atto della sempre più sfumata distinzione tra PII e non-PII al fine di adottare un approccio normativo più efficace ed esaustivo[846], gli ALI *Data Principles*, pur optando per una nozione

[839] D.J. SOLOVE, P.M. SCHWARTZ, ALI Data Privacy: Overview and Black Letter Text, 68, *UCLA Law Review*, 2020 disponibile su *ssrn.com*, 13.

[840] Definiti come "*sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners*". CAL. CIV. CODE §§ 1798.140 (c)(1).

[841] CAL. CIV. CODE §1798.140 (c).

[842] Si veda, ad esempio, la disciplina delle *consumer proprietary network information* (CPNI) dettata in ambito di telecomunicazioni, la disciplina delle *protected health information* di cui allo *Health Insurance Portability and Accountability Act*, ovvero la disciplina degli *education records* di cui al *Family Educational Rights and Privacy Act*. Cfr. P.M. SCHWARTZ, D.J. SOLOVE, Reconciling Personal Information in the U.S. and EU, *Cal. L. Rev*., 2014, 877, 882-890.

[843] Articolo 4 para 1 n.1 GDPR. Sulla riconducibilità dell'indirizzo IP alla nozione di dato personale si veda anche la sentenza della Corte di Giustizia dell'Unione europea (Seconda Sezione) del 19 ottobre 2016 nel caso Causa C-582/14, *Patrick Breyer contro Bundesrepublik Deutschland* ECLI:EU:C:2016:779.

[844] Sulla difficoltà di individuare una nozione uniforme di "*personal identifiable informati*on" e le conseguenti incertezze sul regime di tutela apprestato ai dati personali negli Stati Uniti si veda P.M. SCHWARTZ, D. J. SOLOVE, Reconciling Personal Information in the United States and European Union, 102, *California Law Review*, 4, 2014, 877ss.

[845] CAL CIV. CODE § 1798.140(o)(1).

[846] *Protecting Consumer Privacy in an Era of Rapid Change* (FEDERAL TRADE COMMISSION, marzo 2012), 18-19.

onnicomprensiva di dato personale, hanno assoggettato le informazioni "identificabili" ad un regime di tutele meno restrittivo. Ciò in quanto, notano i responsabili del progetto, riconoscere diritti quali, ad esempio, quelli di accesso ad informazioni soltanto astrattamente riferibili ad una persona fisica identificata, oltre a porre oneri sproporzionati in capo ai titolari, avrebbe anche il controproducente effetto di disincentivare gli sforzi di pseudonimizzazione[847].

Guardando più nel dettaglio la disciplina dettata dal CCPA, invece, le "*personal information*[848]*"* sono definite come "inf*ormation that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*[849]*."* A tal riguardo, degno di nota è il riferimento che il legislatore californiano, nell'esemplificare le categorie di informazioni ricomprese in tale nozione, opera rispetto alle inferenze estrapolate da informazioni personali al fine di creare profili rappresentativi delle preferenze, caratteristiche, attitudini psicologiche, predisposizioni, comportamenti, intelletto e abilità dei consumatori[850] (salvo si tratti di cc.dd. *deidentified*[851] o *aggregated information*[852]). Tale puntualizzazione, infatti, è particolarmente rilevante con riguardo alle conclusioni raggiunte nel precedente capitolo e, di conseguenza, al fine di meglio delineare i confini di una possibile spiegazione significativa. Una siffatta previsione normativa, infatti, ove replicata nell'ordinamento eurounitario, renderebbe superflue le riflessioni in precedenza condotte circa la configurabilità di segreti commerciali sulle conoscenze inferite da dati personali dai titolari del trattamento, primi fra tutti i profili creati a fini di marketing personalizzato. Ciò in quanto, includendo tali metadati nella nozione di dato personale diverrebbe impossibile negare agli interessati l'accesso a tali informazioni, così come il diritto alla

[847] *Principles of Law, Data Privacy* §2 (c).

[848] In generale, sulle difficoltà incontrate nell'ordinamento statunitense in punto di definizione del concetto di "*personal indentifiable information*" si veda P.M. SCHWARTZ, D.J. SOLOVE, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86, *N.Y.U. L. Rev.*, 2011, 1814ss.

[849] CAL. CIV. CODE §1798.140 (o)(1).

[850] CAL. CIV. CODE §§ 1798.140 (k).

[851] Intesi come dati che non possono "ragionevolmente" identificare, relazionarsi con, descrivere, essere suscettibili di associazione con, o essere ricollegati, direttamente o indirettamente, ad uno specifico consumatore nella misura in cui l'imprenditore che li utilizza: (i) adotti misure tecniche idonee a impedirne la re-identificazione; (ii) implementi prassi aziendali che specificamente ne vietano la re-identificazione e (iii) ne prevengono accidentali fughe; e (iv) non compia alcun tentativo di re-identificazione (cc.dd. *deidentified information*). CAL. CIV. CODE §§ 1798.140 (h).

[852] Definite come informazioni che si riferiscono ad un gruppo o a una categoria di consumatori e dalle quali è stato rimosso ogni riferimento all'identità dei singoli consumatori interessati in modo tale da non essere più ragionevolmente ricollegabili agli stessi o ai loro nuclei familiari. CAL. CIV. CODE §§ 1798.145 (a) (5) e §§ 1798.140 (a).

portabilità degli stessi, con notevoli ripercussioni anche in punto di concorrenza fra le imprese.

Altra importante eccezione riguarda l'inapplicabilità del CCPA ai trattamenti di dati relativi ai propri dipendenti effettuati da datori di lavoro. Parte della dottrina riconduce tale esclusione ad un concepimento legislativo della disciplina più in termini di tutela della trasparenza che non di protezione dei dati personali[853]. Scelta, questa, non condivisa dai redattori degli *ALI Data Privacy Principles* che, al contrario, regolano trattamenti di dati condotti non soltanto nel contesto di attività di offerta di beni e servizi, ma anche nella organizzazione e svolgimento di attività di lavorativa e, quindi, anche ove posti in essere da datori di lavoro[854].

Dal punto di vista dell'ambito territoriale di applicazione, a dispetto del silenzio degli ALI *Data Privacy Principles*, il CCPA delimita la sua portata ai trattamenti effettuati almeno in parte in California evitando la riproduzione di più radicali meccanismi di extraterritorialità assimilabili a quelli di cui all'articolo 3 GDPR che, nell'ordinamento statunitense, avrebbero finito per tradursi in intollerabili ed illegittime ingerenze nel commercio interno degli altri Stati[855].

In particolare, la prima obiezione potrebbe essere mossa ai sensi della c.d. *Dormant Commerce Clause*: dottrina di matrice giurisprudenziale volta a invalidare legislazioni statali aventi effetti discriminatori verso attori che operano al di fuori del singolo Stato interessato[856]. Ai sensi di tale disciplina, infatti, ove anche la legislazione

[853] N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37, 43.

[854] *Principles of Law, Data Privacy* §1 (c).

[855] Nelle parole del legislatore californiano: "*commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California*." CAL. CIV. CODE §§ 1798.145 (a) (6). Per riflessioni sul rapporto tra l'aterritorialità della rete e il GDPR si veda A. BARLETTA, La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di internet, *Europa e diritto privato*, 4, 2017, 1179ss; A.G. STANZIONE, Il regolamento europeo sulla privacy: origini e ambito di applicazione, *Europa e Diritto Privato*, 4, 2016, 1249ss; L. VALLE, L. GRECO, Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale, *Diritto dell'Informazione e dell'Informatica*, 2, 2017, 168ss.

[856] Per una attenta riflessione sulla costituzionalità del CCPA alla luce della *Dormant Commerce Clause* si veda R. SPIVAK, Too Big a Fish in the Digital Pond: The California Consumer Privacy Act and the Dormant Commerce Clause, 88, *U. Cin. L. Rev.*, 2020, 475, 493ss. Cfr. J.L. GOLDSMITH, A.O. SYKES, The Internet and the Dormant Commerce Clause, 110, *The Yale Law Journal*, 5, 2001, 785, 788-89; E.

introdotta non fosse "*facially discriminatory*" sarebbe comunque soggetta al c.d. "*Pike balancing test*"[857] consistente nel verificare se la normativa: (i) preveda un ambito di applicazione omogeneo; (ii) persegua uno scopo legittimo; (iii) produca effetti che incidentalmente si ripercuotono sul commercio inter-statale; (iv) bilanci adeguatamente gli svantaggi causati a livello extra-statale con proporzionati presunti benefici locali[858]. Infine, a prescindere dall'esito di tale test, una siffatta legislazione statale potrebbe comunque essere invalidata ove produca l'effetto pratico di incidere e controllare condotte realizzate al di fuori dei confini dello Stato[859].

Sottoponendo la disciplina del CCPA a tale plurimo vaglio di costituzionalità, la dottrina tende a ritenere superato il c.d. *Pike test*. Nessun dubbio, infatti, può essere invocato circa il carattere imparziale della disciplina, la cui portata è identica tanto nei confronti degli operatori statali, quanto nei confronti di quelli extra-statali. Altrettanto innegabile è il carattere legittimo dello scopo perseguito, soprattutto alla luce della rilevanza primaria riconosciuta dal legislatore californiano al diritto alla privacy, definito "*a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution*[860]*".* Quanto al terzo elemento, sebbene siano state sollevate perplessità in dottrina, non si ritiene che gli effetti prodotti sugli operatori extra-statali possano qualificarsi come componente principale della normativa, la quale mira a dettare regole di condotta a tutela dei propri residenti, con conseguente prevalente e principale attenzione alla condotta degli operatori che operano nel territorio statale e soltanto in via residuale e, per l'appunto incidentale, sugli altri

---

WESLEY CAMPBELL, But It's Written in Pen: The Constitutionality of California's Internet Eraser Law, 48, *Colum. J.L. & Soc. Probs*, 2015, 583; N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37, 48.

[857] Si tratta di un test sviluppato dalla Corte Suprema nella persona del Giudice Stewart nel caso *Pike v. Bruce Church, Inc*., 397 U.S. 137(1970), al fine di arginare l'imposizione di vincoli legislativi sul commercio interstatale tali da porre oneri sproporzionati in capo alle imprese.

[858] Cfr. A.M. PETRAGNANI, The Dormant Commerce Clause: On Its Last Leg, 57, *ALB. L. Rev*., 1994, 1215; S.J. ASTRINGER, The Endless Bummer: California's Latest Attempt to Protect Children Online is Far Out(side) Effective, 29, *Notre Dame J.L. Ethics & Pub. Pol'y* , 2015, 271.

[859] Cfr. M. URSUL, The States' Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause, 52, *Suffolk U. L. Rev*., 2019, 577ss.

[860] La norma prosegue peraltro mettendo in luce come "(a) *The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies*. (b) *The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information*. (c) *In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits*." CAL. CIV. CODE § 1798.1.

soggetti[861]. Analoghe perplessità, tuttavia, sono state formulate con riferimento all'ultimo step del *Pike test*. Il carattere lacunoso del CCPA, infatti, ha indotto parte della dottrina a ritenere i vincoli posti in capo alle imprese potenzialmente sproporzionati rispetto ai ridotti benefici concretamente apportati ai consumatori[862].

Ciononostante, ove anche tale obiezione fosse superata, le ripercussioni transfrontaliere generate dal CCPA sulla condotta di tutti gli operatori che, pur collocati al di fuori della California, vogliano raccogliere dati di residenti ovvero condurre attività (inclusa la compravendita di dati) con operatori ivi stanziati, potrebbero comunque supportare sospetti di incostituzionalità dell'apparato normativo in quanto avente l'effetto pratico di controllare condotte poste in essere al di fuori di confini dello Stato[863]. È pur vero, però, che le menzionate soglie dimensionali introdotte dal CCPA, limitando l'applicazione della disciplina alle sole imprese di maggiori dimensioni o la cui attività consista quasi esclusivamente nel trattamento dei dati, rende inverosimile ritenere che i business interessati fossero precedentemente esenti da qualsivoglia vincolo di *data privacy*.

Spostando l'attenzione al contenuto sostanziale della disciplina introdotta dal CCPA, la dottrina tende a tripartirne il contenuto in profili di "*stewardship*" (presupposti e condizioni per la raccolta dei dati), "*balance of harms*" (valutazione costi-benefici per la definizione dei mezzi e delle finalità del trattamento) e "*redressability*" (rimedi a disposizione degli interessati danneggiati da violazioni commesse dal titolare del trattamento)[864].

Quanto al primo profilo, la raccolta di dati personali è generalmente legittimata dal consenso raccolto attraverso l'accettazione delle *privacy policies* sottoposte all'utente che accede alla pagina web del prestatore del servizio[865]. Quella del regime delle basi

[861] In senso contrario N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37, 50.

[862] Così N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37, 50.

[863] *Healy v. Beer Inst., Inc*., 491 U.S. 324, 336 (1989) 336.

[864] N.F. III PALMIERI, Data Protection in an Increasingly Globalized World, 94, *Ind. L.J*., 2019, 297, 298-306. Per una più complessa suddivisione della disciplina si vedano le cinque categorie elaborate da F.H. CATE, *Big Data, Consent, and the Future of Data Protection*, in C.R. SUGIMOTO, H.R. EBIKA, M.MATTIOLI (a cura di), *Big Data is not a Monolith*, MIT Press, Cambridge (MA), 2016, 4.

[865] Cfr. J.P. NEHF, Incomparability and the Passive Virtues of Ad Hoc Privacy Policy, 76, *U. Colo. L. Rev*., 2005, 1, 4ss.

giuridiche del trattamento, infatti, è una delle più marcate differenze tra l'ordinamento eurounitario e quello statunitense in punto di *data privacy*. Tale difficoltà di armonizzazione è riconducibile alla menzionata matrice costituzionale assunta dalla libertà di trattamento dei dati personali negli Stati Uniti in quanto particolare declinazione del più generale principio di libera circolazione delle informazioni di cui al Primo emendamento[866]. In quest'ottica si giustifica tanto il silenzio del CCPA in punto di basi giuridiche per il trattamento dei dati personali, quanto l'esclusione dalla sfera di operatività degli ALI *Data Privacy Principles* di informazioni "*seeking to promote public understanding or discussion, or data activities that are intended to support such communications, including data activities connected with libraries, archives, journalism, public commentary, scholarship, blogging, biography, satire, or the arts; or the public exchange of publicly available information, except insofar as such exchange is made for particular purposes that would justify the application of these Principles and is consistent with the First Amendment*[867]*."*

Ciononostante, seppure limitatamente ai cc.dd. trattamenti secondari dei dati personali, un passo verso una maggiore armonizzazione della disciplina delle basi giuridiche del trattamento è stato comunque compiuto dagli ALI *Data Privacy Principles*. In particolare, trattamenti "*unrelated to those stated in the notice to individuals pursuant to Principle 4 without the consent of the individual*" sono stati subordinati non soltanto alla specifica prestazione del consenso degli interessati ma anche, alternativamente, al rispetto di una delle altre condizioni tassativamente individuate, quali l'esecuzione del contratto, il rafforzamento della tutela della salute e della sicurezza, ovvero il perseguimento di un interesse legittimo del titolare valido, tuttavia, solo rispetto a trattamenti che non richiedono una *heightened notice*, sul cui regime si dirà di più a breve[868].

---

[866] Sul punto si veda meglio quanto già detto *supra sub* Cap. I par. 1.6. P.M. SCHWARTZ, K.N. PEIFER, Transatlantic Data Privacy Law, 106, *Geo. L.J.*, 2017, 115, 134ss; C.J. COLE, N. COULSON, California V. GDPR: Compare and Contrast (*Wolters Kluwer Legal Insights,* 20 settembre 2018).

[867] *Principles of Law, Data Privacy* §1(b)(2)(E) & (F). Cfr. D.J. SOLOVE, P.M. SCHWARTZ, ALI Data Privacy: Overview and Black Letter Text, 68, *UCLA Law Review*, 2020 disponibile su *ssrn.com*, 7.

[868] Più specificatamente, il paragrafo 5 degli *ALI Data Privacy Principles* stabilisce che "*[p]ersonal data activities may be conducted without consent if*: (1) *the personal data activity is required by law*; (2*) obtaining consent would be impermissible under law*; *or* (3) *obtaining consent would be impractical, or too costly or difficult and the use satisfies one or more of the following criteria*: (A) *the personal data activity is necessary in the performance of a contract to which the data subject is a party*; (B) *the personal data activity significantly advances the protection of the health or safety of the data subject or other people*; (C) *the personal data activity significantly advances protection against criminal or tortious*

Al di là di tale isolato ravvicinamento, tuttavia, i confini di legalità del trattamento dei dati negli Stati Uniti vengono generalmente definiti attraverso la disciplina dei doveri informativi. In questo senso, infatti, si è orientato il legislatore californiano che, col CCPA, ha posto in capo a tutti i soggetti rientranti nella descritta nozione di *business* obblighi di notifica *ex ante* volti a rendere edotti gli interessati delle categorie di informazioni raccolte, delle finalità di utilizzo delle stesse, nonché di eventuali modifiche rispetto a quanto precedentemente comunicato[869].

Tale opzione normativa si inquadra nel modello di *notice-and-consent* che, a partire dagli anni '90 si è diffuso negli USA allo scopo di contemperare l'assenza di un generale divieto di trattamento dei dati personali con il rafforzamento dei livelli di trasparenza e consapevolezza degli interessati nella cessione degli stessi[870]. Tuttavia, analogamente al consenso informato di matrice eurounitaria[871], anche l'efficacia del modello di *notice-and-consent* ha sofferto delle difficoltà di contemperamento tra le istanze di comprensibilità degli interessati e quelle di esaustivo tecnicismo delle Autorità di vigilanza (c.d. "*fundamental dilemma of notice*")[872].

La riflessione dottrinaria scaturitane ha indotto l'ALI a riformare il regime declinandolo in un triplice livello di doveri informativi, il primo dei quali è rappresentato dal c.d. *transparency statement*: dichiarazione di stampo onnicomprensivo e dettagliato indirizzata ad una pletora di tecnici ed esperti del settore e rispondente a esigenze di responsabilizzazione e vigilanza sulle prassi aziendali[873]. Il secondo livello, invece, è quello della c.d. *regular individual notice* in cui è confluita la funzione informativa delle tradizionali *privacy policies*, seppure arricchita di più puntuali vincoli di semplicità e sinteticità strumentali al superamento dei noti fenomeni di *over-information*[874]. Il terzo e

activity by a data subject; (D) *the personal data activity significantly advances the public interest, and it would not pose a significant risk of material harm sufficient to trigger heightened notice pursuant to Principle 4(e); or* (E) *the personal data activity serves a significant legitimate interest, and it neither poses a significant risk of material harm to the data subject or others, nor is significantly unexpected, as is defined in § 4(e)(1)*." *Principles of Law Data Privacy* §5(i).

[869] CAL. CIV. CODE §§ 1798.100. (b).

[870] D.J. SOLOVE, Privacy Self-Management and the Consent Dilemma, 126, *Harv. L. Rev*., 2013, 1880, 1992.

[871] Si veda, ad esempio, P.H. SCHUCK, Rethinking Informed Consent, 103, *Yale L.J*., 1994, 899; N.F. III PALMIERI, Data Protection in an Increasingly Globalized World, 94, *Ind. L.J.*, 2019, 297, 298-306; A.J. MCCLURG, A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98, *Nw. U. L. Rev*., 2003, 63, 133-37.

[872] Cfr. P.M. SCHWARTZ, The EU-US Privacy Collision, 126, *Harv. L. Rev*., 2013, 1966, 1976.

[873] *Principles of Law, Data Privacy* §3(b).

[874] Sul ruolo cruciale della trasparenza nella disciplina dei modelli predittivi automatizzati si veda T.Z. ZARSKY, Transparent Predictions, *U. Ill. L. Rev*., 2013, 1503ss; M. ANNANY e K. CRAWFORD, Seeing

più innovativo livello informativo è quello della c.d. "*hightened notice*", consistente in avvisi interattivi somministrati in forma di *pop-up* all'utenza ogni qualvolta stia per iniziare un trattamento dei dati "*significantly unexpected*" ovvero "*potentially harmful*". In altri termini, l'avvio di trattamenti che l'interessato non potrebbe ragionevolmente prevedere dalla natura del suo rapporto con il titolare del trattamento, ovvero di trattamenti che presentano rischi significativi (perché altamente probabili o perché altamente dannosi) per la sfera giuridica degli interessati, viene ad essere accompagnato da specifici doveri di notifica[875]. Le *heightened notices*, quindi, rievocando le riflessioni compiute in punto di *contextual integrity*[876], si contraddistinguerebbero dalle notifiche individuali tradizionali sia per la tempistica che per le modalità di messa in evidenza del messaggio interattivo, entrambe progettate per massimizzare la capacità dell'informativa di attirare l'attenzione degli interessati in modo più efficace e mirato[877].

Particolare accento sul ruolo che la dimensione formale può svolgere nell'efficientamento degli obblighi informativi[878] è posto anche dal CCPA che, pur non riproponendo la tripartizione del regime di notifica teorizzato negli ALI *Data Privacy Principles*, tenta di agevolare l'esercizio del diritto di opposizione alla vendita dei propri dati personali disponendo l'inclusione di un "*clear and conspicuous link*" nella pagina iniziale del sito *web* di ogni *business* recante la dicitura "*Do Not Sell My Personal*

Without knowing: limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 973-989; S. PAGLIANTINI, Trasparenza contrattuale (voce), in *Enc. Dir.*, Annali VI, 2012, § 12; R. MOMBERG, *Standard Terms and Transparency in Online Contracts*, cit., 201; M. HILDEBRANDT, The Dawn of a Critical Transparency Right for the Profiling Era, in J. BUS, M. CROMPTON, M. HILDEBRANDT, G. METAKIDES (a cura di), *Digital Enlightenment Yearbook 2012*, IOS Press, Amsterdam, 47.

[875] *Principles of Law, Data Privacy* §4(e). Per una prospettiva europea sul problema si veda R. BORNSCHEIN, L. SCHMIDT, E. MAIER, The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: the Example of Cookie Notices, 39, *Journal of Public Policy & Marketing*, 2, 2020, 135ss.

[876] Sulla necessità di rafforzare il peso che le aspettative ragionevoli degli interessati circa le finalità e le modalità di trattamento dei propri dati, specialmente in mancanza di un chiaro quadro normativo, si veda quanto detto *supra sub §* 3.5.

[877] Per riflessioni sulla necessità di ripensare le modalità di somministrazione delle cc.dd. *privacy notices* si veda M. RYAN CALO, Against Notice Skepticism in Privacy (and Elsewhere), 87, *Notre Dame L. Rev*., 2012, 1027. Sulle tradizionali obiezioni mosse alla soluzione del *notice-and-consent* puro si veda, fra gli altri, O. BEN-SHAHAR, C. SCHNEIDER, *More Than You Want To Know: The Failure Of Mandated Consent*, Princeton University Press, Princeton, 2014, 10 e S.E. GINDIN, Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears, 8 *Nw. J. Tech. & Intell. Prop*., 2009, 1, 5.

[878] N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37, 43.

Information[879]*."* Ciò risponde tanto all'esigenza di meglio focalizzare l'attenzione degli interessati sulla possibilità che i propri dati personali siano venduti[880], quanto alla necessità di rendere nota ed intuitiva l'azione necessaria ad impedire tale evenienza (c.d. "*right to opt-out*")[881].

Tale premura legislativa si giustifica alla luce della scarsa attenzione generalmente prestata dagli interessati alla protezione dei propri dati personali, perché inconsapevoli delle modalità di utilizzo o vendita degli stessi[882], ovvero perché motivati dal carattere sostanzialmente indispensabile di molti dei servizi accessibili nella rete, in cambio dell'accesso ai quali difficilmente verrebbe negato il consenso alla vendita delle proprie informazioni[883]. Per questa ragione, il legislatore californiano ha predisposto un'ulteriore salvaguardia allo sforzo proattivo compiuto dall'interessato che ha esercitato il diritto di *opt-out*, vietando agli imprenditori di sottoporre nuove richieste di consenso alla vendita dei suoi dati personali per i dodici mesi successivi[884]. Maggiori cautele sono state inoltre apprestate per il trattamento di dati personali relativi a soggetti minori di tredici anni, rispetto ai quali vige un divieto assoluto di vendita, temperato per gli infra-sedicenni dal consenso esplicito dei genitori. Tale regime di divieto/*opt-in*, tuttavia, ancora una volta

[879] CAL. CIV. CODE §§ 1798.135 (a) (1). Cfr. A.C. RAUL, C.C. FRONZONE e S.S. TAPIA, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 416 ss.

[880] Più specificatamente, gli imprenditori impegnati nella compravendita di dati personali sono tenuti a notificare agli interessati non soltanto la generica possibilità che i propri dati vengano venduti a terzi e il loro diritto di opporsi a tale regime, ma anche le categorie di dati venduti a terzi, nonché le categorie degli acquirenti stessi. CAL. CIV. CODE §§ 1798.120. (b) e §§ 1798.115. (a) (2).

[881] Ai sensi del CCPA il c.d. "*right to opt-out*" è disciplinato attraverso la previsione per cui "[*a*] *consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information*." CAL. CIV. CODE §§ 1798.120. (a). Cfr. J.P. NEHF, Incomparability and the Passive Virtues of Ad Hoc Privacy Policy, 76, U. *Colo. L. Rev.*, 2005, 1, 4ss. Per una posizione critica sull'efficacia del Sistema di *opt-out* si veda anche R.C. WILLIAMS, Due Process, Class Action Opt Outs, and the Right Not to Sue, 115, *COLUM. L. Rev.*, 2015, 599, 615.

[882] Cfr. N. RICHARDS, W. HARTZOG,, The Pathologies of Digital Consent, 96 *Wash. U. L. Rev*., 2019, 1461.

[883] Sulla "*take-it-or-leave-it basis*" si veda N. RICHARDS, W. HARTZOG., The Pathologies of Digital Consent, 96 *Wash. U. L. Rev*., 2019, 1461ss. Cfr. T. BALABAN, Comprehensive Data Privacy Legislation: Why Now is the Time, 1, *Case W. Res. J.L. Tech. & Internet*, 2009, 1, 24; A.C. BORDER, Untangling the Web: an Argument for Comprehensive Data Privacy Legislation in the United States, 35, *Suffolk Transnat'l L. Rev*., 2012, 363ss. . Utile, ai fini di una migliore comprensione delle problematiche inerenti la prestazione online del consenso, è la differenza tra i cc.dd. "*clickwrap agreements*", nei quali la prestazione del consenso è frutto di comportamenti sostanzialmente automatici e non ponderati, e i casi di "*browsewrap websites*" nei quali la prestazione del consenso è ritenuta implicitamente prestata per il tramite della continuata navigazione nel sito web. Cfr. M.A. LEMLEY, Terms of Use, 91 *Minn. L. Rev.*, 2006, 459, 466 (2006); A.M. MATWYSHYN, Privacy, the Hacker Way, 87, *S. Cal. L. Rev*., 2013, 1, 62; K. MCMAHON, Tell the Smart House to Mind Its Own Business: Maintaining Privacy and Security in the Era of Smart Devices, 86, *Fordhaml. Rev*., 2018, 2511, 2536.

[884] CAL. CIV. CODE §§ 1798.135 (a) (5).

viene affievolito dall'attenuato livello di responsabilità degli imprenditori, sanzionabili soltanto a fronte della prova della loro "*actual knowledge*" della minore età degli interessati i cui dati sono stati venduti[885].

Infine, a ulteriore salvaguardia della validità del consenso prestato espressamente o implicitamente (attraverso il mancato esercizio del diritto di *opt-out*), ed a differenza di quanto soltanto implicitamente disposto dal GDPR per effetto della previsione del carattere libero del consenso[886], il CCPA prevede espressamente che "[*a*] *business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by*: (A) *denying goods or services to the consumer*; (B) *charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;* (C) *providing a different level or quality of goods or services to the consumer;* (D) *suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services*[887]*."* Ciò non significa, tuttavia, che all'imprenditore sia sempre proibito riconoscere incentivi economici o di altra natura (incluso un diverso livello qualitativo dei prodotti o servizi offerti) al fine di "stimolare" la prestazione del consenso degli utenti al trattamento e alla vendita dei propri dati. Al contrario, il legislatore californiano ha chiaramente ammesso tali pratiche con l'unico limite della natura iniqua, irragionevole, coercitiva o usuraria delle stesse[888], lasciando così aperta la menzionata strada ermeneutica del consenso (*rectius* dato) come controprestazione, oggetto di recente dibattito nella dottrina italiana[889].

Spostando l'attenzione sugli altri due aspetti del *balance of harms* e della *redressability*, e iniziando dal primo, il CCPA è rimasto sostanzialmente silente in punto di tecniche di bilanciamento dei rischi connessi a prassi aziendali fondate sul trattamento

[885] CAL. CIV. CODE §§ 1798.120. (c).
[886] Considerando 42-43 e articolo 7 GDPR.
[887] CAL. CIV. CODE §§ 1798.125. (a) (1).
[888] In particolare, il CCPA consente espressamente che "[*a*] *business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data."* CAL. CIV. CODE §§ 1798.125. (b) (1) e (4).
[889] Sulle riflessioni sviluppate dalla dottrina italiana circa la natura giuridica del consenso e del dato personale in ottica negoziale, quale oggetto di controprestazione non pecuniaria si veda quanto detto supra sub Cap. I § 1.6.

dei dati personali degli utenti[890]. La mancanza di chiare regole di condotta e standard di sicurezza in punto di *data security*, già rilevata in sede di analisi del ruolo ricoperto dalla FTC in ambito di protezione dei dati personali[891], rimane quindi una delle lacune legislative più problematiche dell'ordinamento statunitense[892]. Le doglianze dei titolati circa l'incertezza dei criteri di adeguatezza da seguire nell'implementazione dei propri sistemi di sicurezza, infatti, sono state solo in parte sopite dalla recente introduzione del *NIST Cybersecurity Framework* recante una serie di standards (peraltro non vincolanti) a guida delle prassi aziendali di *data security*[893].

Siffatto *trend* di vaghezza legislativa è stato inoltre confermato dagli *ALI Data Privacy Principles* nei quali, pur recependo la previsione dell'obbligo di adozione di adeguate misure di sicurezza in capo ai titolari[894], si è ancora una volta omessa la puntuale declinazione degli standard di adeguatezza, rimettendo invece alle Corti e alla FTC, in qualità di Autorità competente a svolgere funzioni di vigilanza in materia di *data privacy*, la definizione degli stessi su base più casistica[895]. Tale soluzione, ritengono i redattori dei principi, pur potendo generare maggiore incertezza negli operatori, impone atteggiamenti più cauti e proattivi da parte degli stessi, consentendo allo stesso tempo alla normativa di mantenersi flessibile e adeguata all'evoluzione tecnologica[896]. Più specifica, invece, la

[890] S.J. HYMAN, G.R. WALSER-JOLLY, E. FARRELL, What Is a "Reasonable Security Procedure And Practice" Under the California Consumer Privacy Act's Safe Harbor?, 73 *Consumer Fin. L.Q. Rep*., 173, 181ss.

[891] Vedi meglio supra sub § 3.8.1.

[892] Parte della dottrina ritiene che questa soluzione non tenga in adeguata considerazione le esigenze di prevenzione, piuttosto che di repressione, poste dall'implementazione di prassi aziendali aventi ad oggetto lo sfruttamento di dati personali degli utenti. Così N.F. III PALMIERI, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J*., 2020, 37. Per la posizione di chi ritiene, invece, che la concorrenza di mercato sia una sufficiente forza incentivante di condotte virtuose in punto di trattamento dei dati si veda M. BURDON, Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws, 27, *Santa Clara Computer High Tech. L.J*., 2011, 63ss.

[893] M.P. BARRETT, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018) (noto come *NIST Cybersecurity Framework*) disponibile su *www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11*. Cfr. J. KOSSEFF, *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020, 17ss.

[894] *Principles of Law, Data Privacy* §11(b)(1).

[895] Tale approccio di *laissez-faire* si è ripercosso anche sul regime di *accountability* che, declinato in obblighi di puntale documentazione del processo di implementazione di misure di sicurezza informatica nonché delle valutazioni compiute in fase di definizione delle finalità e dei mezzi di trattamento di dati, è comunque subordinato ad una valutazione casistica condotta dall'Autorità di vigilanza di sede di accertamento della correttezza dell'operato dei titolari. *Principles of Law, Data Privacy* §13(d). Cfr. P. BREUNING, Accountability, 10, *Bna World Data Protection Report*, 2010, 1; W. HARTZOG, *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, Harvard, 2018, 94ss; A.E. WALDMAN, Designing Without Privacy, 55, *Houston L.Rev*., 2018, 659ss.

[896] D.J. SOLOVE, P.M. SCHWARTZ, ALI Data Privacy: Overview and Black Letter Text, 68, *UCLA Law Review*, 2020 disponibile su *ssrn.com*, 24.

disciplina dei doveri di notifica in caso di *data breach*, originariamente introdotta in una normativa californiana del 2003 e attualmente vigenti (seppure con termini e regimi parzialmente divergenti) in ciascuno dei 50 Stati[897].

Infine, al di là dell'aspetto della *data security*, altrettanto sintomatica della difficoltà del legislatore statunitense di bilanciare l'introduzione di uno specifico regime di *data privacy* con le più sentite esigenze economiche di sfruttamento pieno delle potenzialità del mercato dei dati personali è la disciplina del diritto alla cancellazione dei dati. Quest'ultimo, concepito come una potenziale forma di censura e limitazione al diritto di libera manifestazione del pensiero di cui al Primo emendamento[898], è stato completamente omesso dagli ALI *Data Privacy Principles* e sottoposto ad una serie particolarmente consistente di eccezioni dal CCPA. In particolare, il legislatore californiano ha previsto la possibilità per i *businesses* di evitare di ottemperare le richieste di cancellazione ove le informazioni personali siano necessarie: (i) a completare una transazione, fornire un bene o un servizio richiesto dal cliente ovvero prevedibile e coerente alla sua relazione con l'imprenditore ovvero per dare esecuzione al contratto; (ii) a individuare, prevenire o reprimere attacchi alla sicurezza informatica; (iii) a individuare o risolvere malfunzionamenti del sistema; (iv) a rispettare gli obblighi di legge imposti dal *California Electronic Communications Privacy act*; (v) a condurre attività di ricerca scientifica, storica, statistica nel pubblico interesse; (vi) ad esercitare il diritto di libera manifestazione del pensiero o altri diritti riconosciuti dall'ordinamento; (vii) ad adempiere un obbligo di legge; (viii) a consentire un trattamento esclusivamente interno delle informazioni per finalità coerenti alle aspettative sviluppate dai consumatori con riguardo alla propria relazione con l'imprenditore; (ix) a utilizzare i dati personali del consumatore internamente all'organizzazione aziendale, in modo rispettoso del contesto

[897] I *data breach*es sono definiti come "*access, acquisition, use, modification, disclosure, or loss of personal data in an unauthorized manner that compromises the privacy or security of the personal data*." *Principles of Law, Data Privacy* §11(b)(1).

[898] Ai sensi della giurisprudenza inaugurata dalla Corte Suprema in *Central Hudson Gas & Electric v. Public Service Commission of New York* 447 U.S. 557 (1980) il bilanciamento tra i doveri di protezione dei dati personali imposti dal CCPA e la tutela costituzionale riconosciuta al *commercial speech* deve tener conto del carattere legittimo o meno dell'attività che va ad incidere su quest'ultimo, dell'esistenza di un sostanziale interesse pubblico alla regolamentazione, dell'idoneità di quest'ultima a perseguire siffatto interesse, nonché del carattere proporzionato della legislazione, che non deve eccedere quanto strettamente necessario al raggiungimento di suddetto interesse. Più in generale sul rapporto tra privacy e primo Emendamento si veda, *ex multis*, *Sorrell v. IMS Health, Inc*., 564 U.S. 552 (2011) e *Wollschlaeger v. Governor, State of Florida*, 848 F.3d 1293 (11th Cir. 2017). Cfr. J.M. BALKIN, Lecture, Information Fiduciaries and the First Amendment, 49, *U.C. Davis L. Rev*., 2016, 1183ss. Vedi anche *supra sub* Cap. I § 1.6.

normativo e coerente al contesto in cui il consumatore ha fornito le proprie informazioni (c.d. "*internal use exception*")[899].

Quanto al terzo e ultimo tema della *redressability*, rilevata la mancanza di sufficiente consenso dottrinale sul punto, l'ALI ha ritenuto opportuno lasciare aperta ogni strada, limitandosi a dettare delle linee guida per l'individuazione di rimedi che siano "*effective, proportionate, and dissuasive*[900]*."* Allo scopo, nell'individuazione delle misure correttive più adeguate, si invita a tener conto di eventuali accordi esistenti tra le parti, della gravità della violazione, del carattere intenzionale o negligente della stessa, della misura dell'arricchimento ingiustamente conseguito dal convenuto, così come dell'esigenza di misure con efficacia deterrente verso potenziali analoghe condotte future[901]. Inoltre, nel quantificare la dannosità della violazione, l'ALI raccomanda l'adozione di una c.d. "*sliding scale*" che, facendo proprio l'insegnamento recentemente ribadito dalla FTC[902], attribuisce alla probabilità del verificarsi del danno una rilevanza proporzionalmente inversa alla gravità dello stesso[903].

Dal canto suo, anche il CCPA, nel riconoscere il diritto degli interessati ad ottenere il risarcimento del danno cagionatogli da trattamenti illeciti dei propri dati personali, ha chiarito che, nel quantificarne l'ammontare, il giudice dovrebbe prendere in considerazione la natura, la gravità e la durata della condotta, il numero di violazioni, l'intenzionalità delle stesse nonché la capacità finanziaria del convenuto[904]. Tuttavia, la scelta del legislatore californiano di subordinare l'esercizio di tale azione alla notifica scritta del consumatore con cui, indicando puntualmente le disposizioni di cui si lamenta la violazione, concede all'impresa un termine di trenta giorni per adottare azioni correttive, ripristinare la conformità alla normativa e notificare per iscritto la circostanza agli interessati, ha suscitato forti perplessità in dottrina. Ciò in quanto in tal modo si verrebbe ad ostacolare l'accesso alla tutela giurisdizionale, consentita soltanto ove

[899] CAL. CIV. CODE §§ 1798.105. (d) (1)-(9).

[900] *Principles of Law, Data Privacy* §14(a).

[901] *Principles of Law, Data Privacy* §14 (c).

[902] Si veda quanto rilevato *supra sub* § 3.8.1 nell'analizzare la posizione assunta dalla FTC nel recente caso LabMD.

[903] *Principles of Law, Data Privacy* §14 (d). Sulle caratteristiche dei danni prodotti da illegittimo trattamento di dati personali si veda, fra gli altri, D.J. SOLOVE, D. KEATS CITRON, Risk and Anxiety: A Theory of Data-Breach Harms, 96, *Tex. L. Rev*., 2018, 737ss.

[904] CAL. CIV. CODE §§ 1798.150. (a) (1). Cfr. A.C. RAUL, C.C. FRONZONE e S.S. TAPIA, *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 2019, 416ss.

l'imprenditore commetta condotte in ulteriore violazione di quanto dichiarato in sede di risposta alla notifica degli interessati[905].

In conclusione, nonostante le indubbie affinità rilevate nell'analisi della disciplina sostanziale dettata dal CCPA e dagli ALI *Data Privacy Principles*, si ritiene opportuno sottolineare che, per quanto apprezzabile sia stata l'iniziativa del legislatore californiano, l'introduzione di una normativa di *data privacy* al mero livello statale è insufficiente a colmare le lacune create dai sovraordinati interventi settoriali compiuti dal legislatore federale, peraltro fatti espressamente salvi dal CCPA che esclude, ad esempio, dal proprio ambito di applicazione informazioni coperte, fra gli altri, dal *Fair Credit Reporting Act*[906]. Tale puntualizzazione lascia quindi presumere che il percorso di affermazione di una disciplina trans-settoriale e onnicomprensiva in punto di protezione dei dati personali non condurrà, perlomeno nel breve periodo, il legislatore statunitense a dotarsi di un regime di tutele equivalenti a quelle dettate dagli artt. 13-15 e 22 GDPR circa il diritto ad una spiegazione (*rectius* comprensibilità) dei processi decisionali automatizzati. Tale conclusione è ulteriormente avallata dal silenzio degli ALI *Data Privacy Principles* sul punto, sintomatico di una propensione legislativa a lasciare inalterato il complesso delle parziali tutele normative e giurisprudenziali ricavabili dai descritti doveri informativi di cui all'ECPA, al FCRA, all'ECOA e, in via residuale, dalla *Due Process Clause*, salvo eventuali interventi della FTC in esercizio della propria potestà di *Magnuson-Moss rulemaking.*

[905] Da notare, tuttavia, che tale ulteriore passaggio preliminare non è richiesto ove il consumatore abbia sofferto danni pecuniari. Così CAL. CIV. CODE §§ 1798.150. (b).

[906] CAL. CIV. CODE §§ 1798.145 (e). Cfr. S.L. PARDAU, 'The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States', 23, *J Tech L & Pol'y*, 2018, 68ss.

CONCLUSIONI

L'ISTITUZIONALIZZAZIONE DELLA TRASPARENZA ALGORITMICA AD OPERA DELL'*ARTIFICIAL INTELLIGENCE ACT*

L'indagine compiuta si è posta l'obiettivo di mettere in luce i molteplici livelli in cui si articola il diritto ad una spiegazione dei processi decisionali automatizzati, tanto a livello domestico quanto in ottica comparatistica. L'analisi dell'articolo 22 GDPR, infatti, presuppone necessariamente una piena consapevolezza delle tematiche informatiche sottese alle varie caratteristiche e declinazioni dei sistemi di intelligenza artificiale che, a loro volta, aprono diversi scenari applicativi con altrettanto diversificati scenari giuridici di riferimento.

Tale pluralità di possibili angoli visuali del fenomeno emerge in modo evidente dalla rassegna del quadro normativo e giurisprudenziale statunitense, dove la frammentarietà legislativa, per quanto a tratti inevitabilmente lacunosa, mette bene in luce l'ampiezza delle questioni giuridiche potenzialmente sottese all'impiego di processi decisionali automatizzati e al diritto/necessità di poterne conoscere la logica di fondo. Dalla disciplina del monitoraggio automatizzato del contenuto di comunicazioni elettroniche, alla formulazione algoritmica di giudizi in punto di valutazione del merito creditizio, alla multiforme potenzialità discriminatoria degli algoritmi indirettamente prodotta dall'implementazione di processi decisionali automatizzati nei settori più disparati: dal *marketing* alle assunzioni, passando per la dislocazione territoriale del personale[907].

Allo stesso modo, anche la rassegna dei più recenti sviluppi legislativi mette in evidenza l'esigenza di una disciplina trasversale in grado di abbracciare e porre un substrato normativo di riferimento su cui poggiare tutti gli impianti legislativi che si

[907] Cfr. W. GREGORY VOSS, Obstacles to Transatlantic Harmonization of Data Privacy Law in Context, *U. Ill. J.L. Tech. & Pol'y*, 2019, 405 ss; A. KELLY-LYTH, Challenging Biased Hiring Algorithms, *Oxford Journal of Legal Studies*, 1 ss; J. GACUTAN, N. SELVADURAI, A statutory right to explanation for decisions generated using artificial intelligence, *International Journal of Law and Information Technology*, 28, 2020, 193 ss; E. FALLETTI, Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, *Diritto dell'informazione e dell'informatica*, 2020, 169ss.

innestano nei vari scenari settoriali creati dall'utilizzo di algoritmi di intelligenza artificiale a fini decisionali[908].

In quest'ottica, risalendo ancora a ritroso i temi trattati nell'indagine condotta, anche l'analisi dell'articolo 22 GDPR, se complessivamente considerata, pone chiaramente l'interprete di fronte a problemi multidisciplinari e trasversali. Dall'inquadramento del contesto tecnologico di riferimento, alle implicazioni di proprietà intellettuale sollevate dall'accesso alla logica algoritmica sotteso al diritto ad una spiegazione di decisioni unicamente automatizzate, alla natura giuridica del rapporto che si instaura non solo tra titolare del trattamento e interessato/destinatario della determinazione algoritmica, ma anche e soprattutto tra titolare e dato personale, sia singolarmente considerato che nella sua dimensione "processata". È, infatti, nelle riflessioni condotte in punto di accesso al profilo e allo pseudocodice, così come nella dimensione negoziale assunta dal rapporto titolare-interessato per effetto del venire ad esistenza di una condizione di liceità del trattamento *ex* artt. 6 e 9 GDPR, che si innesta il cuore dei problemi giuridici posti dal diritto ad una spiegazione così come delineato dall'articolo 22 GDPR[909].

E ancora, da tutte le riflessioni condotte, e dalla casistica sollevata dall'impiego dell'intelligenza artificiale a fini decisionali (dal caso del Credito Sociale Cinese alle formule di *credit scoring* di FICO[910]) emerge ancora un *fil rouge* latente ma sempre più centrale nella trattazione dei temi oggetto dell'indagine condotta: la trasversalità delle

[908] Cfr. A.C. BORDER, Untangling the Web: An Argument for Comprehensive Data Privacy Legislation in the United States, 35 *Suffolk Transnat'l L. Rev*., 2012, 363; W. G. VOSS, K. A. HOUSER, Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies, 56, *Am. Bus. L.J*., 2019, 287; S. TOGAWA MERCER, The Limitations of European Data Protection as a Model for Global Privacy Regulation, *AJIL Unbound*, 2020, 20 ss; V.A. HERTZA, Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018, 1707 ss; N.F. PALMIERI III, Data Protection in an Increasingly Globalized World, 94, *Ind. L.J.*, 2019, 297 ss.

[909] Cfr. R. MESSINETTI, La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata, *Contratto e impresa*, 3, 2019, 861ss; G. OLIVI, Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti, *Il diritto industriale*, 2, 2020, 181ss; M. NIŠEVIĆ, Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR, 1, *Global Privacy Law Review*, 2, 2020, 104ss; G. D'IPPOLITO, Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale, *Diritto dell'Informazione e dell'Informatica*, 2020, 635ss; R.D. BROWN, Property ownership and the legal personhood of artificial intelligence, 30, *Information & Communications Technology Law*, 2, 2020, 208ss; A. CARRATTA, Decisione robotica e valori del processo, *Rivista di diritto processuale*, 2, 2020, 491ss.

[910] Cfr. G. ALPA, Code is law: il bilanciamento dei valori e il ruolo del diritto, Contratto e impresa, 2, 2021, 378 ss; C. YONGO ABUNGU, Democratic Culture and the Development of Artificial Intelligence in the USA and China, *The Chinese Journal of Comparative Law*, 2020. 1ss.

problematiche giuridiche sottese all'utilizzo dell'intelligenza artificiale in generale, e delle sue declinazioni operative a fini decisionali, in particolare.

In quest'ottica, non stupisce e anzi trova piena razionalità e coerenza l'ultimo intervento del legislatore europeo sul tema che, con la proposta di Regolamento europeo n. 106/2021, sta tentando di predisporre un quadro armonizzato di regole per l'intelligenza artificiale[911]. Abbandonando, quindi, un'ottica settoriale e assumendo invece un approccio c.d. *risk-based* si è proposta una classificazione dei sistemi di intelligenza artificiale per classi di rischio determinate in ragione dei pericoli posti, tra l'altro, alla dignità umana, al rispetto della vita privata e alla protezione dei dati personali[912].

Trovano quindi nuova razionalità legislativa le riflessioni condotte nel corso dell'indagine circa i multiformi e multisettoriali rischi posti dall'assunzione di decisioni unicamente automatizzate. Si pone, ad esempio, in linea di continuità con quanto osservato, la collocazione dei sistemi di intelligenza artificiale per la valutazione del merito creditizio e il *credit scoring* fra quelli ad alto rischio in quando suscettibili di condizionare l'accesso a risorse finanziarie o altri servizi fondamentali[913]. Allo stesso modo, le criticità sollevate con riferimento alle applicazioni del modello cinese del credito sociale trovano conforto nel divieto di utilizzo di sistemi di intelligenza artificiale da parte di pubbliche amministrazioni o enti pubblici per la valutazione automatizzata dell'affidabilità delle persone fisiche in base ai loro comportamenti sociali o alle loro caratteristiche personali (conosciute o inferite) e tradotta in un *social score* per l'adozione di trattamenti sfavorevoli agli stessi in contesti sociali diversi o non collegati a quelli in

[911] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Bruxelles, 21 aprile 2021) (COM(2021) 206 final) (d'ora in avanti Artificial Intelligence Act). Cfr. M. SIMONCINI, Lo «stato digitale». L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica, *Rivista Trimestrale di Diritto Pubblico*, 2, 2021, 529 ss; M.T. PARACAMPO, *Big Data, algoritmi e tecnologie emergenti: le applicazioni di intelligenza artificiale nei servizi finanziari*, in ID., *Fintech*, Vol. I, II ed., Giappichelli Editore, 2021, 87ss 74; N. RÉBÉ, *Artificial Intelligence: Robot Law, Policy and Ethics*, Leiden, Nijhoff, 2021, 108ss; D.E. HARASIMIUK, T. BRAUN, *Regulating Artificial Intelligence: Binary Ethics and the Law*, New York, Routledge, 2021, *passim*; L. SALES, Algorithms, Artificial Intelligence and the Law, *Judicial Review*, 25, 2020, 46ss; N.A. SMUHA, From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence, 13, *Law, Innovation and Technology*, 2021, 57ss.

[912] Artificial Intelligence Act, Considerando 28.

[913] Artificial Intelligence Act, Considerando 37.

cui i dati sono stati originariamente raccolti oppure per l'applicazione di trattamenti sfavorevoli comunque sproporzionati o ingiustificati[914].

Sebbene i condizionamenti del divieto all'utilizzo dei dati "in contesti diversi" o per trattamenti "sproporzionati" lasci margini di ambiguità suscettibili di aprire spiragli all'ingresso nell'ordinamento europeo di modelli di *social scoring* (rispettosi dei menzionati limiti funzionali ma non per questo meno problematici), le considerazioni che hanno condotto il legislatore europeo a queste conclusioni legislative si collocano in perfetta linea di continuità con le riflessioni condotte nel corso dell'indagine.

A conferma di tale considerazione si pongono inoltre gli obblighi di trasparenza posti in capo agli utilizzatori di sistemi di intelligenza artificiale ad alto rischio. In particolare, collocandosi evidentemente nel solco tracciato dall'articolo 22 GDPR, il legislatore europeo ha imposto che tali sistemi siano progettati e sviluppati in modo da assicurare agli utenti la possibilità di poter interpretare l'*output* prodotto dal sistema automatizzato e di utilizzarlo nel modo appropriato[915]. Allo stesso modo, il Regolamento si è preoccupato di meglio esplicitare quell'approccio umano-centrico e di *human-in-the-loop* assunto nel ripercorrere le varie teorizzazioni in punto di diritto ad una spiegazione, fissando l'obbligo di prevedere una supervisione umana c.d. *in-built* nei sistemi ad alto rischio[916], tale per cui vi sia sempre un operatore umano dotato di competenze, autorità e formazione necessaria a garantire il controllo operativo finale non superabile dalla macchina[917]. In questo senso riecheggiano le considerazioni svolte dal Gruppo di Lavoro Articolo 29 sull'art. 22 GDPR, nella parte in cui escludevano la natura unicamente automatizzata dei trattamenti in cui vi fosse la possibilità di modificare l'*output* a seguito di valutazioni autonome e competenti di un operatore persona fisica[918].

[914] Artificial Intelligence Act, Articolo 5.
[915] Artificial Intelligence Act, Considerando 47 e Articolo 13.
[916] Artificial Intelligence Act, Considerando 48.
[917] Artificial Intelligence Act, Articolo 14.
[918] V. *supra* Cap. II, § 2.2.1. Cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit*, 11 aprile 2017, 23; A. MANTELERO, *Report on Artificial Intelligence: Artificial Intelligence and Data Protection: Challenges and Possible Remedies* (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasburgo, 25 gennaio 2019 (T-PD(2018)09Rev), 8; P. PAŁKA, A. JABŁONOWSKA, H.W. MICKLITZ e G. SARTOR, *Before machines consume the consumers. High-Level Takeaways from the ARTSY Project*, EUI Working papers, 2018 (LAW 2018/12), 13.

Il legislatore europeo sembrerebbe quindi aver escluso, in questo senso, la natura unicamente automatizzata dei sistemi di intelligenza artificiale ad alto rischio, ciononostante prevedendo espressamente per gli stessi degli standard di trasparenza che in tutto e per tutto richiamano le riflessioni dottrinali condotte in punto di diritto ad una spiegazione così come disciplinato dall'articolo 22 GDPR (applicabile, come noto, per le sole decisioni unicamente automatizzate). Non rappresentano, infatti, una novità assoluta quegli obblighi di "effettiva supervisione" che impongono all'operatore umano coinvolto nel monitoraggio di un sistema di intelligenza artificiale ad alto rischio di essere in grado di comprendere a pieno le capacità e i limiti del sistema così da poterne segnalare tempestivamente le anomalie, di evitare fenomeni di *over-reliance* dell'*output* (c.d. *automation bias*), di interpretare correttamente siffatti *output*, potendo anche decidere di non utilizzarli[919].

In conclusione, con tale proposta di un quadro armonizzato di regole per l'intelligenza artificiale il legislatore europeo sembrerebbe aver portato a frutto le riflessioni, i timori e, in buona parte, le teorizzazioni nel tempo sviluppate nel corso del dibattito dottrinale in punto di diritto ad una spiegazione, trasponendone i risultati nel contesto di un quadro normativo (saggiamente) trasversale e perciò idoneo a porre argini legislativi non settoriali al multiforme fenomeno dell'evoluzione operativa dei sistemi di intelligenza artificiale. Per quanto, infatti, il Regolamento lasci impregiudicato il rispetto del GDPR[920] e, quindi, anche dell'articolo 22, i numerosi limiti all'applicazione della fattispecie di divieto ivi disciplinata, rende del tutto opportuna la reiterazione della *ratio* e la più matura (seppur ancora embrionale) esplicitazione degli obblighi di comportamento ivi sottesi al fine di creare un ecosistema normativo in grado di promuovere lo sviluppo di sistemi di intelligenza artificiale sicuri, affidabili e soprattutto trasparenti.

Il percorso d'indagine condotto e corroborato dai recenti sviluppi legislativi rende perciò evidente l'assunto di fondo di tutto lo studio: non può esistere uno sviluppo tecnologico giuridicamente sostenibile che non sia improntato alla trasparenza dei sistemi automatizzati impiegati per prendere decisioni nei confronti dei singoli. La comprensibilità dei processi decisionali automatizzati non può non assurgere a tassello

[919] Artificial Intelligence Act, Articolo 14.
[920] Artificial Intelligence Act, Considerando 41.

fondamentale di quel percorso di trasformazione normativa che, nelle parole del legislatore europeo, dovrebbe caratterizzare il prossimo "*digital decade*"[921] e, a dispetto della scarsa attenzione originariamente suscitata dall'articolo 22 GDPR, oggi la proposta di regolamento sull'intelligenza artificiale e il forte accento agli obblighi di trasparenza ivi posto rende evidente la sempre più crescente presa di consapevolezza del ruolo cruciale dell'accessibilità alla logica e al funzionamento trasparente dei sistemi di intelligenza artificiale nel far sì che non solo il trattamento dei dati personali, ma anche l'utilizzo dei sistemi di intelligenza artificiale che degli stessi si alimentano e attraverso i quali tale trattamento è sempre più spesso condotto, siano al servizio dell'uomo, come ben chiarito dal considerando 4 del GDPR.

[921] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (Bruxelles, 21 aprile 2021) (COM(2021) 206 final), 4.

BIBLIOGRAFIA

ADDANTE, A., La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali, *Giustizia civile*, 4, 2020

ADEBAYO, J., HURLEY, M., Credit Scoring in the Era of *Big Data*, 18, *Yale J.L. & Tech*., 2016

AGRIFOGLIO, G., Risarcimento e quantificazione del danno da lesione della *privacy*: dal danno alla persona al danno alla personalità, 4, *Europa e Diritto Privato*, 2017

ALLEN, A. L., *Uneasy Access: Privacy for Women in a Free Society*, Totowa (NJ), Rowman & Littlefield, 1988

ALLEN, M. e ORHEIM, A., Get Outta My Face[book]: The Discoverability of Social Networking Data and the Passwords Needed to Access Them, 8, *Wash. J. L. Tech. & Arts*, 2, 2012

ALPA, G., *Code is law*: il bilanciamento dei valori e il ruolo del diritto, *Contratto e impresa*, 2, 2021

ALPA, G., *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019

ALPA, G., RESTA, G., *Le persone fisiche e i diritti della personalità*, in R. SACCO (diretto da), *Trattato di diritto civile*, Vol. I, II ed., Torino, Utet, 2019

ALVISI, C., *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

AMORE, G., Fairness, Transparency e Accountability nella protezione dei dati personali, Studium Iuris, 4, 2020

ANANNY, M., e CRAWFORD, K., Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, 20, *New Media & Society*, 3, 2018

ANDOLINA, A., Tutela delle liste clienti tra concorrenza sleale, segreto industriale e banche dati, 5, *Giur. It*., 2018

ANGIOLINI, C., *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Giappichelli Editore, Torino, 2020

ARE, M., Beni immateriali (voce), *Enc. dir*., V, Milano, Giuffré, 1959

ARE, M., L'oggetto del diritto di autore, Milano, Giuffré, 1963

ASCARELLI, T., *Teoria della concorrenza e dei beni immateriali*, III ed., Milano, Giuffré, 1960

ASTRINGER, S.J., The Endless Bummer: California's Latest Attempt to Protect Children Online is Far Out(side) Effective, 29, *Notre Dame J.L. Ethics & Pub. Pol'y* , 2015

AZIZ, S. e DOWLING, M., Machine Learning and AI for Risk Management, in T. LYNN, J.G. MOONEY, P. ROSATI e M. CUMMINS (Eds), *Disrupting Finance: FinTech and Strategy in the 21st Century*, Palgrave Macmillian, Dublino, 2019

BALABAN, T., Comprehensive Data Privacy Legislation: Why Now is the Time, 1, *Case W. Res. J.L. Tech. & Internet*, 2009

BALGANESH, S., Quasi-Property: Like, but not Quite Property, 160, *U. Penn. Law Rev.*, 2012

BALKIN, J.M., Cultural Democracy and the First Amendment, 110, *Nw. U. L. Rev.*, 2016

BALKIN, J.M., Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society, 79, *N.Y.U. L. Rev.*, 2004

BALKIN, J.M., Lecture, Information Fiduciaries and the First Amendment, 49, *U.C. Davis L. Rev.*, 2016

BALKIN, J.M., The First Amendment in the Second Gilded Age, 66, *Buff. L. Rev.*, 2018

BAMBAUER, J., Is Data Speech?, 66, *Stan. L. Rev.*, 2014

BAMBAUER, J.R., The Relationships Between Speech and Conduct, 49, *U.C. Davis L. Rev.*, 2016

BAMBERGER, K.A., MULLIGAN, D.K., Privacy on the Books and on the Ground, 63, *Stan. L. Rev.*, 2011

BANTERLE, F., BLEI, M., Alcune novità introdotte dalla direttiva Trade Secrets, 4, *Diritto industriale*, 2017

BARBAZZA, A., *Natura, contenuto e struttura dei diritti della personalità*, in S. RUSCICA (a cura di), *I diritti della personalità*, Padova, Cedam, 2013

BARCELLONA, M., Attribuzione normativa e mercato sulla teoria dei beni giuridici, *Quadrimestre*, 1987

BARFIELD, W., Towards a Law of Artificial Intelligence, in W. BARFIELD e U. PAGALLO (a cura di), *Research Handbook on the Law of Artificial Intelligence*, Edward Elgar Publishing, Northampton, 2018

BARLETTA, A., La tutela effettiva della privacy nello spazio (giudiziario) europeo e nel tempo (della "aterritorialità") di internet, *Europa e diritto privato*, 4, 2017

BARRAD, C.M.V., Genetic Information and Property Theory, 87, *Nw. U. L. Rev.*, 1993

BARRETT GLASGOW, J., *Data Brokers: Should They Be Reviled or Revered?*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge, Cambridge University Press, 2018

BASUNTI, C., La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali, *Contratto e impresa*, 2, 2020

BATHAEE, Y., The Artificial Intelligence Black Box and the Failure of Intent and Causation, 31, *Harv. J.L. & Tech.*, 2018.

BATTELLI, E., Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi, *Corriere Giur.*, 12, 2019

BATTELLI, E., D'IPPOLITO, G., *Il diritto alla portabilità dei dati*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

BAVETTA, G., Identità (diritto alla), *Enc. dir.*, XIX, Milano, Giuffré, 1970

BEHAR, D.C., An Exception to an Exception: Officer Inadvertence as a Requirement to Plain View Seizures in the Computer Context, 66, *U. Miami L. Rev.*, 2012

BELLOVIN, S.M., HUTCHINS, R.M., JEBARA, T., ZIMMECK, S., When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning, 8, *N.Y.U. J. L. & Liberty*, 2014

BEN-SHAHAR, O. e SCHNEIDER, C.E., *More Than You Wanted to Know. The Failure of Mandated Disclosure*, Princeton University Press, Princeton, 2014

BERLE, I., *Face Recognition Technology. Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal*, Law, Governance and Technology Series, Springer, Cham, 2020

BERLINGIERI, E., *Legge 2.0: il web tra legislazione e giurisprudenza*, Milano, Apogeo, 2008

BERTANI, M., *Proprietà intellettuale, antitrust e rifiuto di licenze*, Quaderni di Aida, X, Milano, Giuffré, 2004

BEWERLY-SMITH, H., Ohly, A., Lucas-Schloette, A., *Privacy, Property and Personality. Civil Law Perspective on Commercial Appropriation*, Cambridge Studies in Intellectual Property Rights, Cambridge, Cambridge University Press, 2005

BIANCHI, L., Il diritto alla portabilità, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

BIFERALI, G., *Big Data* e valutazione del merito creditizio per l'accesso al *peer to peer lending*, 3, *Diritto dell'informazione e dell'informatica*, 2018

BIFULCO, R., La sentenza Schrems e la costruzione del diritto europeo della privacy, in *Giur. Cost.*, 2016

BINKLEY, J.W., Fair Notice of Unfair Practices: Due Process in FTC Data Security Enforcement After Wyndham, 31, *Berkeley Tech. L.J.*, 2016

BIONDI, B., *I beni*, in F. VASSALLI (diretto da), *Trattato di diritto civile italiano*, Vol. IV.1, Torino, 1953

BOERDING, A., CULIK, N., DOEPKE, C., HOEREN, T., JUELICHER, T., ROETTGEN, C., SCHOENFELD, M.V., Data Ownership. A Property Rights Approach from a European Perspective, 11, *Journal of Civil Law Studies*, 2, 2018

BONAVITA, S. (a cura di), *Società delle tecnologie esponenziali e* General Data Protection Regulation*. Profili critici nella protezione dei dati*, Ledizioni LediPublishing, Milano, 2018

BONE, R.G., A New Look at Trade Secret Law: Doctrine in Search of Justification, 86, *Calif. L. Rev*., 1998

BORCHERT, C.J., PINGUELO, F.M., THAW, D., Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act, 13, *Duke L. & Tech. Rev*., 2013

BORDER, A.C., Untangling the Web: an Argument for Comprehensive Data Privacy Legislation in the United States, 35, *Suffolk Transnat'l L. Rev*., 2012

BORGHI, M., *Owning Form, Sharing Content: Natural-Right Copyright in the Digital Environment*, in F. MACMILLAN (a cura di), *New Directions in Copyright Law*, Vol. 5, Cheltenham-Northampton, Edward Elgar, 2007

BORGIA, F., *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

BORNSCHEIN, R., SCHMIDT, L., MAIER, E. , The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: the Example of Cookie Notices, 39, *Journal of Public Policy & Marketing*, 2, 2020

BOYDEN, B.E., Can a Computer Intercept your email?, 34 *Cardozo L. Rev*., 2012

BOYDEN, B.E., *Privacy of Electronic Communications*, in K.J. MATHEWS (a cura di), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age,* II ed., Practicing Law Institute, 2011

BOYNE, S.M., Data Protection in the United States, 66, *Am J Comp L*, 2018

BOYNE, S.M., *Data Protection in the United States: U.S. National Report*, in D. M. VICENTE e S. DE VASCONCELOS CASIMIRO (a cura di), *Data Protection in the Internet*, Ius Comparatum – Global Studies in Comparative Law, Vol. 38, Springer, Cham, 2020

BRANDEIS, L.D. e WARREN, S.D. JR., The Right to Privacy, 4, *Harv. L. Rev*., 5, 1890

BRAUCHER, J., Deception, Economic Loss and Mass-Market Customers: Consumer Protection Statutes as Persuasive Authority in the Common Law of Fraud, 48, *Ariz. L. Rev*., 2006

BRAVO, F., Access to source code of proprietary software used by public administrations for automated decision-making. What proportional balancing of interests?, in *European Review of Digital Administration & Law (Erdal)*, 1-2, 2020

BRAVO, F., *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Cedam, Padova, 2018

BRAVO, F., *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017

BRAVO, F., *L'"architettura" del trattamento e la sicurezza dei dati e dei sistemi*, in C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

BRAVO, F., Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto, 1, *Contratto e impres*a, 2019

BRAVO, F., Trasparenza del codice sorgente e decisioni automatizzate, *Diritto dell'Informazione e dell'Informatica*, 4, 2020

BRENNAN, L., The Public Policy of Information Licensing, 36, *Hous. L. Rev*., 1999

BRENNAN-MARQUEZ, K., "Plausible Cause": Explanatory Standards in the Age of Powerful Machines, *70, Vanderbilt Law Review, 2017*

BRENNAN-MARQUEZ, K., Fourth Amendment Fiduciaries, 84, *Fordham L. Rev*., 2015

BRESLIN, J., *False Light: The Tortured and Troubled Tort That Survives*, in W.A. BABCOCK e W.H. FREIVOGEL (a cura di), *The SAGE Guide to Key Issues in Mass Media Ethics and Law*, Vol. 2, Los Angeles, Sage Publishing, 2015

BREUNING, P., Accountability, 10, *Bna World Data Protection Report*, 2010

BRILL, J., *The intersection of Privacy and Consumer Protection*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018

BRKAN, M., Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond, 11, *International Journal of Law and Information Technology*, 2019

BRUEGGEMANN WARD, K., The Plain (or Not So Plain) View Doctrine: Applying the Plain View Doctrine to Digital Seizures, 79, *University of Cincinnati Law Review*, 3, 2011

BURDON, M., Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws, 27, *Santa Clara Computer High Tech. L.J*., 2011

BURRELL, J., How the machine 'thinks': understanding opacity in machine learning algorithms, 3, *Big Data & Society*, 1, 2016

BUSIA, G., Diritto alla riservatezza (voce), *Digesto*, 2000

BUTERA, A., *Il Codice civile italiano. Libro della proprietà*., I, Torino, 1941

BUTLER, H.N., WRIGHT, J.D., Are State Consumer Protection Acts Really Little-FTC Acts?, 63, *Fla. L. Rev*., 2011

BYGRAVE, L.A., *Data privacy law: an international perspective*, Oxford University Press, Oxford, 2014

BYGRAVE, L.A., *Data protection law: approaching its rationale, logic and limit*s, Kluwer Law International, Alphen aan den Rijn, 2002

BYGRAVE, L.A., Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling, 17, *Computer Law & Security Report*, 2001

BYGRAVE, L.A., Minding the machine: Article 15 of the EC data protection directive and automated profiling, 17, *Comput. Law Secur. Rev*., 1, 2001

CAGGIA, F., *Libertà ed espressione del consenso*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

CAGGIANO, I.A., Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali, *Osservatorio del diritto civile e commerciale*, 1, 2018

CALDERS, T. e CUSTERS, B., What is Data Mining and How Does it Work? in B. CUSTERS, T. CALDERS, T., SCHERMER, B. e ZARSKY, T. (a cura di), *Discrimination and Privacy in the Information Society*. *Data Mining and Profiling in Large Databases*, Springer, New York, 2013

CALDERS, T. e ŽLIOBAITĖ, I., *Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society*. *Data Mining and Profiling in Large Databases*, Springer, New York, 2013

CALDERS, T., ŽLIOBAITĖL, I., Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures, in B. CUSTERS, T. CALDERS, B. SCHERMER, T. ZARSKY (a cura di), Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases, Springer, New York, 2013

CALISAI, F. , *I diritti dell'interessato*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

CALO, M.R., The Boundaries of Privacy Harm, 86, *Ind. L.J*., 2011

CAMARDI, C., Cose, beni e nuovi beni, tra diritto europeo e diritto interno, 3, *Europa e diritto privato*, 2018

CAMARDI, C., Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/1996, 4, *Europa e diritto privato*, 1998

CAMARDI, C., Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali, in *Giustizia civile*, 2019

CAMARDI, C., Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali, 3, *Giustizia Civile*, 2019

CAMARDI, C., TABARRINI, C., *Contact tracing* ed emergenza sanitaria. ''Ordinario'' e ''straordinario'' nella disciplina del diritto al controllo dei dati personali, 3, *La Nuova Giurisprudenza Civile Commentata*, 2020

CARIDI, G., Introduzione alla elaborazione automatica dei dati per le decisioni economiche e finanziarie, Napoli, ESI, 1995

CARLONI, E., I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo, in *Diritto Amministrativo*, 2, 2020

CARNELUTTI, F., *Usucapione della proprietà industriale*, Milano, Giuffré, 1938

CARPENTER, D., *Autonomy (of Individuals and Private Associations)*, in M. TUSHNET, M.A. GRABER, S.LEVINSON (a cura di), *The Oxford Handbook of the U.S. Constitution*, Oxford, Oxford University Press, 2015

CASEY, B., FARHANGI, A., VOGL, R., Rethinking Explainable Machines: the GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise, 34, *Berkeley Tech. L.J.*, 2019

CASTELLANO, J.M., *Prosecutor's Manual for Arrest, Search and Seizure*, III ed., New York, LexisNexis, 2015

CATE, F.H., *Big Data* consent and the future of data protection in C.R. SUGIMOTO, H.R. EBIKA, M.MATTIOLI (a cura di), *Big Data is not a Monolith*, MIT Press, Cambridge (MA), 2016

CAVANI, G., *Oggetto della tutela*, in L.C. UBERTAZZI (a cura di), *Legge sul software. Commentario sistematico*, Quaderni di Aida, I, Milano, Giuffré, 1994

CERRATO, S.A., Appunti su *Smart Contract* e diritto dei contratti, *Banca Borsa Titoli di Credito*, 3, 2020

CHANDER, A., GELMAN, L., RADIN, M.J. (a cura di), *Securing Privacy in the Internet Age*, Standford University Press, Standford, 2008

CHURCH, P., MILLARD, C., Comments on the data protection directive, in A. BÜLLESBACH, S. GIJRATH, Y. POULLET, C. PRINS (a cura di), Concise European IT law, 2 ed., Kluwer Law International, Alphen aan den Rijn, 2010

CIAN, G., Pagamento (voce), *Dig. Disc. Priv.*, Sez. civ., XIII, Torino, 1995

CIANI, J., Property Rights Model v. Contractual Approach: How Protecting Non-Personal Data in Cyberspace?, *Diritto del Commercio Internazionale*, 4, 2017

CICCONE G. e GHINI, F., La tutela giudiziale civile dei segreti commerciali anche dopo l'introduzione del d.lgs. n. 63/2018, 5, *Diritto industriale*, 2019

CITRON, D.K., Technological due process, 85, 2007

COFONE, I.N., *Privacy Tradeoffs in Information Technology Law*, Erasmus University, 2015

COGLIANESE, C., D. LEHR, Transparency and Algorithmic Governance, 71 *Admin. L. Rev*., 2019

COHEN, J.E., The Regulatory State in the Information Age, 17, *Theoretical Inquiries L*., 2016

COLAPIETRO C., e IANNUZZI, A., *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO e C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale scientifica, Napoli, 2017

COMPORTI, M., *Diritti reali in generale*, in A. CICU, F. MESSINEO, L. MENGONI, (già diretto da) e P. SCHLESINGER (continuato da), *Trattato di diritto civile e commerciale*, II ed., Milano, Giuffré, 2011

COSTA, P., Diritti fondamentali (storia dei) (voce), *Enc. dir*., II, Milano, Giuffré, 2008

COTTINO, G., *Diritto commerciale*, I, Padova, Cedam, 1976

COUTURE, S., *The Ambiguous Boundaries of Computer Source Code and Some of Its Political Consequences*, in J. VERTESI, D. RIBES (a cura di), *digitalSTS: A Field Guide for Science & Technology Studies*, Princeton University Press, Princeton, 2019

CRANE, C., Social Networking v. the Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking, 89, *Wash. U. L. Rev*., 2012

CRAWFORD, K. e SCHULZ, J. , *Big Data* and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55, *Boston College Law Rev*, 93, 2014

CRESPI, G., commento *sub* artt. 98-99 c.p.i, in A. VANZETTI (a cura di), Codice proprietà industriale, Milano, Giuffrè, 2013

CROWTHER, B.T., (Un)Reasonable Expectation of Digital Privacy, 2012, *Brigham Young University Law Review*, 1, 2012

CUFFARO, V., *Il diritto europeo sul trattamento dei dati personali e la sua applicazione*, 2019

CUFFARO, V., *Profili introduttivi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

CUOCCI, V., Fornitura di contenuti digitali e controprestazione non pecuniaria: luci e ombre sulla tutela del consumatore nella prospettiva del diritto contrattuale europeo, in F. DI CIOMMO, O.

TROIANO (a cura di), Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido, Studi in onore di Roberto Pardolesi, Piacenza, 2018

CUSTERS, B.H.M., Predicting Data that People Refuse to Disclose; How Data Mining Predictions Challenge Informational Self- Determination, *Privacy Observatory Magazine*, 3, 2012

CUSTERS, B.H.M., URSIC, H., Big Data and data re-use: a taxonomy of data re-use for balancing Big Data benefits and personal data protection, 6, *International Data Privacy Law*, 2016

D'ACQUISTO, G. e NALDI, M. *Big Data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Giappichelli Editore, Torino, 2017

D'AGOSTINO, A., *Il sistema di gestione della privacy*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

D'IPPOLITO, G., Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale, in *Diritto dell'Informazione e dell'Informatica*, 3, 2020

D'IPPOLITO, G., Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale, *Diritto dell'Informazione e dell'Informatica*, 2020

D'IPPOLITO, G., Il principio di limitazione della finalità del trattamento tra *data protection* e antitrust. il caso dell'uso secondario di *Big Data*, 6, *Diritto dell'informazione e dell'informatica*, 2018

DANIEL MITTELSTADT, B., ALLO, P., TADDEO, M., WACHTER S., e FLORIDI, L., The Ethics of Algorithms: Mapping the Debate, 2, *Big Data & Society*, 2016

DASKAL, J., Microsoft Ireland, the Cloud Act, and International Lawmaking 2.0, 71, *Stan. L. Rev. Online*, 2018

DATTA, A., SEN S., ZICK Y., *Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems* (PROCEEDINGS OF THE 2016 IEEE SYMPOSIUM ON SECURITY & PRIVACY), 2016

DAVIES, S.G., Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in P.E. AGRE, M. ROTENBERG (a cura di), *Technology & Privacy*, Cambridge (MA), MIT Press, III ed., 2001

DAVIS, S., The False Promise of Fiduciary Government, 89, *Notre Dame L. Rev.*, 2014

DE BERNART, M., *La videosorveglianza e il controllo del lavoratore*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

DE CUPIS, A., *I diritti della personalità*, in A. CICU, F. MESSINEO, L. MENGONI, (già diretto da) e P. SCHLESINGER (continuato da), *Trattato di diritto civile e commerciale*, II ed., Milano, Giuffré, 1982

DE FRANCESCHI, A., *Il "pagamento" mediante dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, 1389

DE FRANCESCHI, A., Il "pagamento" mediante dati personali, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

DE FRANCESCHI, A., *La circolazione dei dati personali tra privacy e contratto*, Edizioni Scientifiche Italiane, Napoli, 2017

DE FRANCESCHI, A., The EU Digital Single Market Strategy in Light of the Consumer Rights Directive, 4, *Journal of European Consumer and Market Law*, 4, 2015

DE GREGORIO, G., TORINO, R., *Privacy, protezione dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

DE HERT, P., PAPAKONSTANTINOU, V., MALGIERI, G. , BESLAY, L., SANCHEZ, I., The right to data portability in the GDPR: Towards user-centric interoperability of digital services, 34, *Computer Law & Security Review*, 2, 2018

DE LEONARDIS, F., Big data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione, in E. CALZOLAIO (a cura di), *La decisione nel prisma dell'intelligenza artificiale*, Padova, Wolter Kluwers Cedam, 2020

DE MEO, R., Autodeterminazione e consenso nella profilazione dei dati personali, *Dir. Inf.*, 2013

DE SANCTIS, V., Considerazioni giuridiche sulla riforma della legislazione sul diritto d'autore, *Il diritto di autore*, 1940

DE SANCTIS, V.M., *I soggetti del diritto d'autore*, II ed., Milano, Giuffrè, 2005

DE SEMO, G., *Istituzioni di diritto privato*, V ed., Firenze, G. Barbèra, 1948

DE STEFANI, F., *Le regole della privacy. Guida pratica al nuovo GDPR*, Ulrico Hoepli Editore, Milano, 2018

DE VRIES, K. e HILDEBRANDT, M., Introducing Privacy, Due Process and the Computational Turn at a Glance: Pointer for the Hurried Reader, in ID. (a cura di), *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology*, Routledge, New York, 2013

DEITEL, H. M., DEITEL, P.J., *C++. Fondamenti di programmazione*, Maggioli Editore, 2014

DEL FEDERICO, C., POPOLI, A.R., *Disposizioni generali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017

DEMOTT, D.A., Beyond Metaphor: An Analysis of Fiduciary Obligation, *Duke LJ*, 1988

DESTRI, I. e LOTTO, A.M., *La profilazione*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

DETERMANN, L., No One Owns Data, 70, *Hastings L.J.*, 1, 2018

DI LORENZO, G., *Spunti di riflessione su taluni "diritti dell'interessato"*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019

DI MAJO, A., *Delle obbligazioni in generale*. *Art. 1173-1176*, Bologna, Zanichelli, 1988

DI RESTA, F., *La nuova 'Privacy europea': i principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Giappichelli Editore, Torino, 2018

D'IPPOLITO, G., INCUITTI, E.M., I processi decisionali interamente automatizzati nel settore assicurativo, in *Rivista di diritto dell'impresa*, 3, 2019, 735-752

DIVER, C.S., The Optimal Precision of Administrative Rules, 93 *Yale L. J.*, 1983

DOBKIN, A., Information Fiduciaries in Practice: Data Privacy and User Expectations, 33, *Berkeley Tech. L.J.*, 2018

DOGGRELL, K., *Checking Out: What the Rise of the Sharing Economy Means for the Future of the Hotel Industry*, Bloomsbury, Londra, 2020

DOMINO, J.C., *Civil Rights and Liberties in the 21st Century*, IV ed., New York, Routledge, 2018

DOW SCHÜLL, N., Self in the Loop: Bits, Patterns, and Pathways in the Quantified Self, in Z. PAPACHARISSI (a cura di), *A Networked Self and Human Augmentics, Artificial Intelligence, Sentience*, Routledge, New York, 2019

DREXL, J., Designing Competitive Markets for Industrial Data. Between Propertisation and Access, 8, *JIPITEC*, 2017

DURST, L., *Oggetto e finalità: un nuovo statuto giuridico dei dati personali*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

EASTERLY, W., *The Tyranny of Experts. Economists, Dictators, and the Forgotten rights of the Poor*, Basic Books, New York, 2014

EDWARDS, L. e VEALE, M., Enslaving the algorithm: from a "right to an explanation" to a "right to better decisions"?, 16, *IEEE Security & Privacy*, 3, 2018

EDWARDS, L. e VEALE, M., Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16, *Duke Law & Technology Review*, 18, 2017

ELVY, S.A., Paying for privacy and the personal data economy, 117, *Columbia Law rev.*, 6, 2017

ETZIONI, A., *The Limits of Privacy*, New York, Basic Books, 1999

EZRACHI, A. e STUCKE, M., *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Boston, Harvard University Press, 2016

FAINI, F., *Big Data e* Internet of Things*:* Data Protection *e* Data Governance *alla luce del regolamento europeo,* in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

FALCE, V., Dati e segreti. Dalle incertezze del Regolamento Trade secret ai chiarimenti delle Linee Guida della Commissione UE, 2, *Diritto industriale*, 2018

FALCE, V., GHIDINI, G., OLIVIERI, G. (a cura di), *Informazione e big data tra innovazione e concorrenza*, Milano, Giuffré, 2017

FALLETTI, E., Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, *Diritto dell'informazione e dell'informatica*, 2, 2020

FALLETTI, E., Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche, in *Diritto dell'Informazione e dell'Informatica*, 2020

FALLON, R.H. Jr., The Linkage Between Justiciability and Remedies — And Their Connections to Substantive Rights, 92 *Va. L. Rev*., 2006

FARACE, D., Le persone autorizzate al trattamento dei dati personali, *Rivista Trimestrale di Diritto e Procedura Civile*, 2, 2021

FARACE, D., 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, Giuffré, 2019

FARINA, M. , *I contratti informatici*, Milano, Editore Key, 2018

FAVILLI, C., *La nozione di discriminazione tra normativa comunitaria e leggi italiane*, in G. DE MARZO (a cura di), *Il codice delle pari opportunità*, Giuffré editore, Milano, 2007

FAYYAD, U., PIATETSKY-SHAPIRO, G. e SMYTH, P., From Data Mining to Knowledge Discovery in Databases, 17, *AI Magazine*, 3, 1996

FERRAJOLI, L., *Diritti fondamentali. Un dibattito teorico*, Roma, Editori Laterza, 2001

FERRARA, L., *Il diritto reale di autore in rapporto alla nuova legge italiana*, Napoli, Jovene, 1940

FERRARI, M., L'uso degli algoritmi nell'attività amministrativa discrezionale, in *Il diritto degli affari*, 1, 2020

FERRI, G.B., *Persona e formalismo giuridico*, Rimini, Maggioli Editore, 1987

FEUER, L.S., Who is Poking Around Your Facebook Profile? The Need to Reform the Stored Communications Act to Reflect a Lack of Privacy on Social Networking Websites, 40, *Hofstra Law Review*, 2, 2011

FIETKIEWICZ, K.J., HENKEL, M., *Privacy Protecting Fitness Trackers: An Oxymoron or Soon to be Reality?*, in G. MEISELWITZ (a cura di), *Social Computing and Social Media. User Experience and Behavior*, Vol. I, Springer International Publishing, Cham, 2018

FINK, K., Opening the government's black boxes: freedom of information and algorithmic accountability, 21, *Information, Communication & Society*, 10. 2018

FINKELMAN, P., *The Encyclopedia of American Civil Liberties: A - F, Index*, New York, Routledge, 2006

FINOCCHIARO, G., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in ID. (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017

FINOCCHIARO, G., La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems, in *Dir. Inf. E inform*., 2015

FINOCCHIARO, G., *Sistema di diritto industriale*, Vol. I, Padova, Cedam, 1932

FISHER III, W.W., Property and Contract on the Internet, 73, *Chi.-Kent L. Rev*., 1998

FLANAGAN, O.J., *Science of the Mind*, 2 ed., MIT Press, Massachusetts, 1991

FORD, M.V., Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology, 19*, American University Journal of Gender Social Policy and Law*, 4, 2011

FRANCESCHELLI, R., *Beni immateriali*, Torino, Utet, 1960

FRANCESCHELLI, R., L'oggetto del rapporto giuridico, *Riv. Trim. dir. proc. civ*., 1957

FRAU, R., *Il trattamento dei dati personali nell'attività bancaria*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

FREEDMAN, W., *The Right of Privacy in the Computer Age*, New York, Quorum Books, 1987

FREIWALD, S., First Principles of Communications Privacy, *Stan. Tech. L. Rev*. 3, 2007

FRIED, C., Privacy, 77, *Yale L.J.*, 1968

FRIGNANI, A., Segreti d'impresa (voce), *Digesto*, IV, Disc. Priv. Sez. Comm., vol. XIII, 1997

FROOMKIN, A.M., Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements, *U. Ill. L. Rev.*, 2015

FUMAGALLI, G., *La tutela del software nell'Unione Europea. Brevetto e diritto d'autore*, Milano, Nyberg Edizioni, 2005

FUNK, W., Public Participation and Transparency in Administrative Law – Three Examples as an Object Lesson, 61, *Admin. L. Rev*., 2009

G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e Normativa Privacy Commentario. Regolamento (UE) 2016/679 del 27 aprile 2016 - Decreto di adeguamento D.Lgs. n. 101/2018 - Codice privacy D.Lgs. n. 196/2003*, Ipsoa, Milano, 2018

GACUTAN, J., SELVADURAI, N., A statutory right to explanation for decisions generated using artificial intelligence, *International Journal of Law and Information Technology*, 28, 2020

GAETA, M.C., La protezione dei dati personali nell'*Internet of Things*: l'esempio dei veicoli autonomi, 1, *Diritto dell'informazione e dell'informatica*, 2018

GALETTA, D.U., Algoritmi, procedimento amministrativo e garanzie: brevi riflessioni, anche alla luce degli ultimi arresti giurisprudenziali in materia, *Rivista Italiana di Diritto Pubblico Comunitario*, 3, 2020

GALGANO, F., *Diritto privato*, XVIII ed., Padova, Cedam, 2019

GALGANO, F., *Trattato di diritto civile*, Vol. I, III ed., Cedam, Padova, 2014

GAMBINI, M., *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

GAVISON, R., Privacy and the Limits of Law, 89, *Yale Law Journal*, 1980

GELLMAN, R. e DIXON, P., *Failures of Privacy Self-Regulation in the United States*, in D. WRIGHT e P. DE HERT (a cura di), *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, Law, Governance and Technology Series 25, Springer, 2016

GENNARI, G., Consenso informato: ritorno all'anno zero, 71, *Responsabilità civile e previdenza*, 9, 2006

GERACI, R.M., La circolazione transfrontaliera delle prove digitali in UE: la proposta di regolamento *E-Evidence*, 3, *Cassazione Penale*, 2019

GERMANI, E., FEROLA, L., Il *wearable computing* e gli orizzonti futuri della *privacy*, 1, *Diritto dell'informazione e dell'informatica*, 2014

GHOSH, S., *How to Build a Commons: Is Intellectual Property Constrictive, Facilitating, or Irrelevant?*, in C. HESS, E. OSTROM (a cura di), *Understanding Knowledge as a Commons. From Theory to Practice*, Cambridge (MA), MIT Press, 2007

GIAMPICCOLO, G., La tutela giuridica della persona umana e il c.d. diritto alla riservatezza, *Riv. trim. dir. e proc. civ*, 2, 1958

GILLESPIE, T., The relevance of algorithms, in T. GILLESPIE, P.J. BOCZKOWSKI, & K.A. FOOT (a cura di), *Media Technologies: Essays on Communication, Materiality, and Society*, MIT Press, Cambridge (MA), 2014

GILLIS, T.B., SPIESS, J.L., *Big Data* and Discrimination, 86, *U. Chi. L. Rev.*, 2019

GINDIN, S.E., Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears, 8 *Nw. J. Tech. & Intell. Prop.*, 2009

GINSBERG, J., MOHEBBI, M.H., PATEL, R.S., BRAMMER, L., SMOLINSKI, M.S., BRILLIANT, L., Detecting influenza epidemics using search engine query data, 457, *Nature*, 2009

GIORGIANNI, M., Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato, *Contratto e impresa*, 4, 2019

GIOVANELLA, F., *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

GIOVANNANGELI, S.F., *L'informativa agli interessati e il consenso al trattamento*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

GIUGGIOLI, P.F., Tutela della privacy e consumatore, in E. TOSI (a cura di), Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy, Milano, Giuffré, 2019

GLUCK, A.R., The Federal Common Law of Statutory Interpretation: Erie for the Age of Statutes, 54, *Wm. & Mary L. Rev.*, 2013

GNESI, S., MATTEUCCI, I., MOISO, C., MORI, P. , PETROCCHI, M. , VESCOVI, M. , *My Data, Your Data, Our Data: Managing Privacy Preferences in Multiple Subjects Personal Data*, in B. PRENEEL, D. IKONOMOU (a cura di), *Privacy Technologies and Policy, Lecture Notes in Computer Science*, Berlino, Springer, 2014

GOIMLEY, K., One Hundred Years of Privacy, *Wisc. L. Rev.*, 5, 1992

GOLDSMITH, J.L., SYKES, A.O., The Internet and the Dormant Commerce Clause, 110, *The Yale Law Journal*, 5, 2001

GOODMAN, B. e FLAXMAN, S., European Union regulations on algorithmic decision-making and a "right to explanation", 38, *AI Magazine*, 3, 2017

GORGONI, M., La "stagione" del consenso e dell'informazione: strumenti di realizzazione del diritto alla salute e di quello all'autodeterminazione, 64, *Responsabilità civile e previdenza*, 1, 1999

GRABER, M.A. e GILLMAN, H., *The Complete American Constitutionalism. Introduction and the Colonial Era*, Vol. I, Oxford, Oxford University Press, 2015

GRAZIANI, A., *Istituzioni di economia politica*, IV ed., 1936

GREENWOOD, D., STOPCZYNSKI, A., SWEATT, B., HARDJONO, T. e PENTLAND, A., *The New Deal on Data*, in T. HARDJONO, D.L. SHRIER, A.PENTLAND (a cura di), *Trusted Data. A New Framework for Identity and Data Sharing*, MIT Press, 2014

GRIMMELMANN, J., The Law and Ethics of Experiments on Social Media Users, 13, *Colo. Tech. LJ*., 2015

GRIMMELMANN, J., WESTREICH, D., Incomprehensible Discrimination, 7, *Calif. L. Rev. Online*, 2016

GRIMMELMANN, J., When All You Have Is a Fiduciary, Law & Pol. Econ., 2019

GROTTO, T., CASADIO, M., *La certificazione dei consensi raccolti* online, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

GUGLIELMETTI, G., *Analisi e decompilazione dei programmi*, in L.C. UBERTAZZI, *La legge sul software. Commentario sistematico*, Quaderni di Aida n.1, Milano, Giuffrè, 1994

GUIDOTTI, R. *et al*., A survey of methods for explaining black box models, 51, *ACM Computing Surveys (CSUR)*, 5, 2018

HACKER, P., Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law, 55, *Common Market Law Review*, 4, 2018

HAGEL III, J., RAYPORT, J.F., The Coming Battle for Customer Information, *Harv. Bus. Rev*., 1997

HALL, K.L. e PATRICK, J.J., *The Pursuit of Justice. Supreme Court Decisions that Shaped America*, Oxford, Oxford University Press, 2006

HARASIMIUK, D.E., BRAUN, T., *Regulating Artificial Intelligence: Binary Ethics and the Law*, New York, Routledge, 2021

HARTZOG, W., *Privacy's Blueprint. The Battle to Control the Design of New Technologies*, Harvard University Press, Harvard, 2018

HARTZOG, W., RICHARDS, N., Privacy's Constitutional Moment and the Limits of Data Protection, 61, *Boston College Law Review*, 2020

HAZAN, T., PAPANDREOU, G., TARLOW, D. (a cura di), *Perturbations, Optimization, and Statistics*, MIT Press, Cambridge (MA), 2016

HELVESTON, M.N., Consumer Protection in the Age of Big Data, 93, *Wash. U. L. Rev*., 2016

HENELIUS, A., *et al*., A Peek into the Black Box: Exploring Classifiers by Randomization, 28, *Data Mining & Knowledge Discovery*, 2014

HENKIN, L., Privacy and Autonomy, 74, *Columbia Law Review*, 7, 1974

HENNIG, C. e MEILA, M., *Cluster Analysis: An Overview*, in C. HENNIG, M. MEILA, F. MURTAGH, R. ROCCI (a cura di), *Handbook of Cluster Analysis*, NW, CRC Press-Taylor & Francis Group, 2016

HERTZA, V.A., Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?, 93, *N.Y.U. L. Rev*., 2018

HETCHER, S., The De Facto Federal Privacy Commission, 19, *J. Marshall J. Computer & Info. L.*, 2000

HILDEBRANDT, M., Law as Computation in the Era of Artificial Legal Intelligence: Speaking Law to the Power of Statistics, 68, *U. Toronto L.J.*, 1, 2018

HILDEBRANDT, M., Location Data, *Purpose Binding and Contextual Integrity: What's the Message?*, in L. FLORIDI (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, Vol. 17, Law, Governance and Technology Series, Springer, Cham, 2014

HILDEBRANDT, M., *Smart Technologies and the End(s) of Law Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Northampton, 2015

HILDEBRANDT, M., The Dawn of a Critical Transparency Right for the Profiling Era, in J. BUS, M. CROMPTON, M. HILDEBRANDT, G. METAKIDES (a cura di), *Digital Enlightenment Yearbook 2012*

HILL, R., What an algorithm is, 29, *Philosophy & Technology*, 1, 2015

HIRSCH, D.D., Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law, 41, *Ga. L. Rev*., 2006

HODNETT, M. e WILEY, J.F., *Deep Learning Essentials*, Packt Publishing, Birmingham, 2018

HOFFMAN, S., *Big Data* and the Americans with Disabilities Act, 68, *Hastings L.J.*, 2017

HOFMANN, M., *Federal Trade Commission Enforcement of Privacy*, in K.J. MATHEWS (a cura di), *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, II ed., Practicing Law Institute, 2011

HURLEY, M. e ADEBAYO, J., Credit Scoring in the Era of *Big Data*, 18 *Yale J.L. & Tech*., 2016

HURWITZ, J., Data Security and the FTC's UnCommon Law, 103, *Iowa L. Rev.*, 2016

HYMAN, S.J., WALSER-JOLLY, G.R., FARRELL, E., What Is a "Reasonable Security Procedure And Practice" Under the California Consumer Privacy Act's Safe Harbor?, 73 *Consumer Fin. L.Q. Rep*., 2020

IASELLI, M., *Intelligenza artificiale e robotica*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

IRTI, C., Dato personale, dato anonimo e crisi del modello normativo dell'identità, 2, *Jus Civile*, 2020

IRTI, N., *Proprietà e impresa*, Napoli, Jovene, 1965

ITALIANO, G.F., *Intelligenza Artificiale: passato, presente e futuro*, in F. PIZZETTI (a cura di), *Intelligenza Artificiale, Protezione dei Dati Personali e Regolazione*, G. Giappichelli Editore, Torino, 2018

J.A. ADAMS e D.D. BLINKA, *Prosecutor's Manual for Arrest, Search and Seizure*, II ed., New York, LexisNexis, 2012

JANECEK, V., MALGIERI, G., Data Extra Commercium, in LOHSSE, S., SCHULZE, R., STAUDENMAYER, D., (a cura di), *Data as Counter-Performance—Contract Law 2.0?*, Hart Publishing/Nomos, 2019

JANEČEK, V., Ownership of Personal Data in the Internet of Things, 34, *Computer L. & Security Rev*., 5, 2018

JANGER, E.J., Privacy, Property, Information Costs, and the Anticommons, *Hastings L.J*., 54, 2003

JOHNSON, O.C.A., The Agency Roots of Disparate Impact, 49, *Harvard Civil Rights-Civil Liberties Law Review*, 2014

KAMMOURIEH, L., BAAR, T., BERENS, J., LETOUZÉ, E., MANSKE, J., PALMER, J., SANGOKOYA, D. e VINCK, P., *Group Privacy in the Age of Big Data*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017

KAMMOURIEH, L., BAAR, T., BERENS, J., LETOUZÉ, E., MANSKE, J., PALMER, J., SANGOKOYA, D. e VINCK, P., *Group Privacy in the Age of Big Data*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017

KAMMOURIEH, L., *Group Privacy in the Age of Big Data,* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017

KANG, J., Self-Surveillance Privacy, 97, *Iowa L. Rev*., 2012

KANOVITZ, J.R., *Consitutional Law for Criminal Justice*, XIV ed., New York, Routledge, 2015

KARNOW, C.E.A., The Encrypted Self: Fleshing Out the Rights of Electronic Personalities, 13, *Journal of Computer & Information Law*, 1994

KASPEREK SOMES, T., Assessing Spokeo, Inc. v. Robins: The Future of Statutory Damage Class Actions in the Consumer Protection Arena, 20, *J. Consumer & Com. L*., 2017

KEATS CITRON, D., e PASQUALE, F., The Scored Society: Due Process for Automated Predictions, 89, *Washington Law Review*, 2014; 126

KEATS CITROW, D., Technological Due Process, 85, *Wash UL Rev*, 2008

KEFFER, S., Too Big to Surveil: The Fourth Amendment Illuminated By 'Modern Lights' and Shadowed By *Obsta Principiis* in a Post-Carpenter World Concerned With Privacy, 2, *Information & Communications Technology Law*, 28, 2019

KERBER, W., *Rights on Data: The EU Communication 'Building a European Data Economy' from and Economic Perspective*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Oxford, Hart Publishing, 2017

KERR, O.S., Fourth Amendment Seizures of Computer Data, 119 *Yale L.J.*, 2010

KERR, O.S., The Curious History of Fourth Amendment Searches, 2012, *The Supreme Court Review*, 2012

KHAN, L.M., POZEN, D.E., A Skeptical View of Information Fiduciaries, 133, *Harvard. L. Rev*., 2019

KIM, P., Data-Driven Discrimination at Work, 58, *Wm. & Mary L. Rev*., 2017

KLITOU, D., *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, Information Technology and Law Series, Vol. 25, Berlino, Asser Press-Springer, 2014

KOCH, C.H. JR., MARTIN, B., FTC Rulemaking through Negotiation, 61, *N.C. L. Rev*., 1983

KOSSEFF, J., *Cybersecurity Law*, II ed., Wiley, Hoboken, 2020

KOZINSKI, A., The Dead Past, 64, *Stan. L. Rev. Online*, 2012

KREIMER, S.F., Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record, 159, *U. Pa. L. Rev*., 2011

KREPS, D.M., Bounded Rationality, 3, *The New Palgrave Dictionary of Economics and the Law*, 1998

KROLL, J.A. *et al*., Accountable algorithms, 165, *University of Pennsylvania Law Review*, 2016

KROLL, J.A., HUEY, J. , BAROCAS, S., FELTEN, E.W., REIDENBERG, J.R., ROBINSON, D.G., YU, H., Accountable Algorithms, *165, University of Pennsylvania Law Review, 2017*

KROTOSZYNSKI, R.J. JR, Back to the Briarpatch: An Argument in Favor of Constitutional Meta-analysis in State Action Determinations, 94, *Mich. L. Rev*., 2, 1995

KROTOSZYNSKI, R.J. JR, *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford, Oxford University Press, 2016

KRYSA, J. e SEDEK, G. , *Source Code*, in M. FULLER (a cura di), *Software studies\ a lexicon*, MIT Press, Cambridge (MA), 2008

KUNER, C., SVANTESSON, D.J.B., CATE, F.H., LYNSKEY, O., MILLARD, C., *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, 7, *Int. Data Priv. Law*, 1, 2017

KURAN, T., *Private Truths, Public Lies: The Social Consequences of Preference Falsification*, Cambridge (MA), Harvard University Press, 1995

LA DIEGA, G.N., Le idee e il muro del suono. I programmi per elaboratore nella più recente giurisprudenza europea, 2, *Europa e dir. Priv*, 2013

LANGHANKE, C., SCHMIDT-KESSEL, M., Consumer data as consideration, in *Journal of European Consumer and Market Law*, 6, 2015, 218-223

LANGHANKE, C., SCHMIDT-KESSEL, M., Consumer Data as Consideration, 4, Journal of European Consumer and Market Law, 6, 2015

LASLETT, P., *Patriarcha and other political works of Sir Robert Filmer*, Oxford, B. Blackwell, 1949

LASSWELL, B.R., In Defense of False Light: Why False Light Must Remain a Viable Course of Action, 34, *Texas Law Review*, 1993

LAUDON, K.C., Markets and Privacy, International Conference on Information Systems, 1993

LEHMANN, M., *A European Market for Digital Goods*, in A. DE FRANCESCHI (a cura di), *European Contract Law and the Digital Single Market. The implications of the Digital Revolution*, Cambridge, Intersentia, 2016

LEIB, E.J., PONET, D.L., SEROTA, M., A Fiduciary Theory of Judging, 101, *Calif. L. Rev*., 2013

LEIGH, K., *Developments on the Fourth Amendment and Privacy to the 21st Century* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015

LEMLEY, M.A., Terms of Use, 91 *Minn. L. Rev.*, 2006

LEMLEY, M.A., The Surprising Virtues of Treating Trade Secrets as IP Rights, 61, *Stanford Law Review*, 2, 2008

LEONARD, M.E., *The Chainging Expectations of Privacy in the Digital Age* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Santa Barbara (CA), ABC-CLIO LLC, 2015

LEPRI, B., STAIANO, J., SANGOKOYA, D., LETOUZÉ, E. e OLIVER, N., The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good, in T. CERQUITELLI, D. QUERCIA, F. PASQUALE (a cura di), *Transparent Data Mining for Big and Small Data*, Studies in *Big Data*, Vol. 11, Berlino, Springer, 2017

LESSING, L., The Architecture of Privacy, 1, *Vand. J. Ent. L. & Prac*., 1999

LETA JONES, M., The right to a human in the loop: Political constructions of computer automation and personhood, 47, *Social Studies of Science*, 2, 2017

LEVI, A., *Teoria generale del diritto*, Padova, Cedam, 1967

LEWANDOWSKI, D. Is Google Responsible for Providing Fair and Unbiased Results?, in M. TADDEO, L. FLORIDI (a cura di), The Responsibilities of Online Service Providers, Law, Governance and Technology Series, Vol. 31, Springer, New York, 2017

LITMAN, J., Information Privacy/Information Property, 52, *Stan. L. Rev*., 2000

LOCKE, J., *Second Treaties of Government*, 1690

LUBBERS, J.S., It's Time to Remove the 'Mossified' Procedures for Removing FTC Rulemaking, 83, *Geo. Wash. L. Rev*. 2015

LUCCHI, N., *I Contenuti Digitali: Tecnologie, Diritti e Libertà*, Springer, 2010

LUCCHINI GUASTALLA, E., Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori, *Contratto e impresa*, 1, 2018

LUCCHINI GUASTALLA, E., *Privacy e Data Protection: principi generali*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

MACCARTHY, M., *In defence of Big Data Analytics*, in E. SELINGER, J. POLONETSKY, O. TENE (a cura di), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, Cambridge, 2018

MACLIN, T., *The Supreme Court and the Fourth Amendment's Exclusionary Rule*, Oxford, Oxford University Press, 2013

MAGELLI, S., Il know-how nell'esperienza giurisprudenziale italiana tra esclusiva e concorrenza sleale, 2, *Diritto Industriale*, 2016

MAGGIOLINO, M., *Big Data* e prezzi personalizzati, 1, *Concorrenza e mercato*, 2016

MAGGIOLINO, M., *EU Trade Secrets Law and Algorithmic Transparency*, AIDA, Milano, Giuffrè, 2018

MAGLIO, M., *Il regolamento europeo 2016/679 in materia di dati personali: inquadramento generale e prospettive di sviluppo*, in M. MAGLIO, M. POLINI, N. TILLI (a cura di), *Manuale di diritto alla protezione dei dati personali*, II ed., Santarcangelo di Romagna, Maggioli Editore, 2019

MAIORCA, C., Beni (voce), *Enc. giur. Treccani*, Vol. V, Roma, 1988

MAIORCA, C., *La cosa in senso giuridico. Contributo alla critica di un dogma*, Napoli, Edizioni Scientifiche Italiane, 1978

MALGIERI G. e COMANDÈ, G., Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation, 7, *International Data Privacy Law*, 4, 2017

MALGIERI, G., "Ownership" of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?, 20, *Journal of Internet Law*, 5, 2016

MALGIERI, G., Pricing Privacy, *Computer law & security review*, 34, 2018

MALGIERI, G., Trade Secrets v Personal Data: a possible solution for balancing rights, *International Data Privacy Law*, 6, 2016

MANENTI, R. e MARZIALE, G., *Delle obbligazioni*, in S. RUPERTO (con il coordinamento di), *La giurisprudenza sul codice civile coordinata con la dottrina. Libro IV delle obbligazioni (artt. 1823-1935)*, Milano, Giuffrè, 2012

MANTEI, C.J., Pornography and Privacy in Plain View: Applying the Plain View Doctrine to Computer Searches, 53, *Ariz. L. Rev*., 2011

MANTELERO, A., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era* in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017

MANTELERO, A., *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, Giuffré, 2007

MANTELERO, A., L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU e USA. Quali scenari per cittadini ed imprese?, in *Contratto e impresa*, 2015

MANTELERO, A., *La privacy all'epoca dei Big Data*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

MANTELERO, A., La privacy all'epoca dei big data, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, 1181-1212

MANTELERO, A., Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, 32, *Computer Law & Security*, 2016

MARGULIS, S.T., *Three Theories of Privacy: An Overview*, in S. TREPTE, L. REINECKE (a cura di), *Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web*, Springer, Berlino, 2011

MARINO, G., *I diritti degli interessati*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

MAROI, F., Cosa (voce), *Nuovo dig. it.*, IV, Torino, Utet, 1938

MARTIN, S.L., Interpreting the Wiretap Act: Applying Ordinary Rules of Transit to the Internet Context, 28, *Cardozo L. Rev*., 2006

MASCETTI, S., MONREALE, A,, RICCI A., e GERINO, A., *Anonymity: A Comparison Between the Legal and Computer Science Perspectives*, in S. GUTWIRTH, L. LEENES, P. DE HERT, Y. POULLET (a cura di), *European Data Protection: Coming of Age*, Dordrecht, Springer, 2013

MASSIMI, M., Quali orizzonti per il marketing?, in R. PANETTA (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018, Milano, Giuffré, 2019

MASTRELIA, D., La tutela del know-how, delle informazioni e dei segreti commerciali fra novità normative, teoria e prassi, 5, *Diritto industriale*, 2019

MATHESON, J. H., The Equal Credit Opportunity Act: A Functional Failure, 21, *Harv. J. On Legis.*, 1984

MATTARELLA, G. , Big Data e accesso al credito degli immigrati: discriminazioni algoritmiche e

MATTASSOGLIO, F., *Big Data*, in M. T. PARACAMPO (a cura di), *FinTech: Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Giappichelli Editore, Torino, 2017

MATTIOLI, M., Disclosing *Big Data*, in *Minnesota Law Review*, 99, 2014

MATWYSHYN, A.M., Privacy, the Hacker Way, 87, *S. Cal. L. Rev*., 2013

MAURO, T., *I Big Data tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

MAYER-SCHONBERGER, V. e RAMGE, T., *Reinventing Capitalism in the Age of Big Data*, John Murray Publishers, Londra, 2018

MAYER-SHÖNBERGER, V., Beyond Privacy, Beyond Right. Toward a 'System' Theory of Information Governance, 98, *Cal. L. Rev*., 2010

MCCLURG, A.J., A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98, *Nw. U. L. Rev*., 2003

MCGEVERAN, W., Friending the Privacy Regulators, 58, *Ariz. L. REV*., 2016

MCINNIS, T.N., *The Evolution of the Fourth Amendment*, Plymouth, Lexington Books, 2010

MCMAHON, K., Tell the Smart House to Mind Its Own Business: Maintaining Privacy and Security in the Era of Smart Devices, 86, *Fordhaml. Rev*., 2018

MCTHOMAS, M., *The Dual System of Privacy Rights in the United States*, New York, Routledge, 2013

MENDOZA, I. e BYGRAVE, L.A., The Right Not to be Subject to Automated Decisions Based on Profiling, in T.E. SYNODINOU, P. JOUGLEUX, C. MARKOU E T. PRASTITOU (a cura di), *EU Internet Law. Regulation and Enforcement*, Springer International Publishing AG, Cham, 2017

MENEGHETTI, M.C., *Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, 2017

MENELL, P.S., LEMLEY, M.A., MERGES, R.P., *Intellectual Property in the New Technological Age*, Vol. I, Clause 8 Publishing, 2019

MESSINETTI, D., Beni immateriali (voce), *Enc. giur. Treccani*, V, Roma, 1988

MESSINETTI, D., Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali, 16, *Riv. crit. dir. priv.*, 3, 1998

MESSINETTI, D., *Oggettività giuridica delle cose incorporali*, Milano, Giuffré, 1970

MESSINETTI, D., Personalità (diritti della) (voce), *Enc. dir.*, XXXIII, Milano, Giuffré, 1983

MESSINETTI, R., *Circolazione dei dati personali e autonomia privata*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019

MESSINETTI, R., La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata, in *Contratto e impresa*, 2019, 3, 861 ss

MIDIRI, M., Le piattaforme e il potere dei dati (Facebook non passa il Reno), in *Diritto dell'Informazione e dell'Informatica*, 2, 2021, 111 ss

MINZNER, M., Why Agencies Punish, 53 *Wm. & Mary L. Rev.*, 2012

MITTELSTADT, B.D., P. ALLO, M. TADDEO, S. WACHTER, L. FLORIDI, *The ethics of algorithms: Mapping the debate*, *Big Data & Society*, 2, 2016

MOLLO, F., *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019

MONAGHAN, M., INGOLD, J., Policy Practitioners' Accounts of Evidence-Based Policy Making: The Case of Universal Credit, *Journal of Social Policy*, 2, 48, 2019, 351 ss

MONTANARO, D., *Il diritto di accesso ai dati personali e il diritto di rettifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

MORAIS CARVALHO, J., Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771, in *EuCML*, 2019, 194 ss

MOSKOVITZ, M., *Cases and Problems in Criminal Procedure: The Police*, V ed., LexisNexis, 2010

MULLIGAN, D.K., Reasonable Expectations in Electronic Communications. A Critical Perspective on The Electronic Communications Privacy Act, 72, *Geo. Wash. L. Rev.*, 2004

MURPHY, R.S., Property Rights in Personal Information: An Economic Defense of Privacy, 84, *Geo. L.J.*, 1996

MUSKIN, V.P., The Right to Be Forgotten, 91, *Mar N.Y. St. B.J.*, 2019

NATOLI, U., *La proprietà*, Milano, Giuffré, II ed., 1976

NAZZARO, A.C., P*rivacy, smart cities e smart cars*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

NEHF, J.P., Incomparability and the Passive Virtues of Ad Hoc Privacy Policy, 76, *U. Colo. L. Rev*., 2005

NERVI, A., *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

NERVI, A., La nozione giuridica di informazione e la disciplina di mercato. Argomenti di discussione, *Riv. dir. comm*., 1998

NICOLÒ, R., *L'adempimento dell'obbligo altrui*, Vol. X, Napoli, Edizioni Scientifiche Italiane, 1978

NIMMER, R.T., Breaking Barriers. The Relation Between Contract and Intellectual Property Law, 13, *Berkeley Tech. L.J*., 1998

NIŠEVIĆ, M., Profiling Consumers Through Big Data Analytics: Strengths and Weaknesses of Article 22 GDPR, 1, *Global Privacy Law Review*, 2, 2020

NISSENBAUM, H., Privacy as Contextual Integrity, 79, Washington Law Review, 1, 2004

NOTO LA DIEGA, G., *Data as Digital Assets. The Case of Targeted Advertising*, in M. BAKHOUM, CONDE GALLEGO, B., MACKENRODT, M.O., SURBLYTE-NAMAVICIENE, G. (a cura di), *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Towards a Holistic Approach*?, MPI Studies on Intellectual Property and Competition Law, Vol. 28, Springer, Berlino, 2018

NUNZIATO, D.C. With Great Power Comes Great Responsibility: Proposed Principles of Digital Due Process for ICT Companies, in L. FLORIDI (a cura di), *Protection of Information and the Right to Privacy - A New Equilibrium?*, Vol. 17, Cham, Springer, 2014

O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Broadway Books, 2016

ODDENINO, A., *Reflection on Big Data and International Law*, 4, *Diritto del Commercio Internazionale*, 2017

OHM, P., The Fourth Amendment in a World Without Privacy, 81, *Miss. L.J*., 2012

OHM, P., The Rise and Fall of Invasive ISP Surveillance, *U. Ill. L. Rev*., 2009

OPPO, G., *Sul consenso dell'interessato*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffré, 1999

OREFICE, M., I *Big Data*. Regole e concorrenza, 4, *Politica del diritto*, 2016

ORESTANO, R., *Azione, diritti soggettivi, persone giuridiche. Scienza del diritto e storia*, Bologna, Il Mulino, 1978

OROFINO, A.G., GALLONE, G., L'Intelligenza Artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione, in *Giur. It.*, 2020, 7, 1738 ss

OROFINO, A.G., GALLONE, G., L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione, in *Giur. it.*, 2020, 1738 ss

OTTOLIA, A., *Big Data* e Innovazione Computazionale, Quaderni di Aida n.28, Torino, Giappichelli Editore, 2017

OVERBECK, W., BELMAS, G., SHEPARD, J., *Major Principles of Media Law*, Cengage Learning, 2017; 208

PACKARD, V., *The Naked Society*, Brooklyn, Ig Publishing, 1964

PAGLIANTINI, S., Contratti di vendita di beni: armonizzazione massima, parziale e temperata della Dir. UE 2019/771, *Giur. It.*, 2020, 1, 217 ss

PAJNO, A., BASSINI, M., DE GREGORIO, G., MACCHIA, M., PATTI, F. P., POLLICINO, O., QUATTROCOLO, S., SIMEOLI, D., SIRENA, P., AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista, *BioLaw Journal - Rivista di BioDiritto*, 3, 2019, 217 ss

PALAZZOLO, G., La banca dati e le sue implicazioni civilistiche in tema di cessione e deposito alla luce del reg. (UE) n. 2016/679, *Contratto e impresa*, 2017

PAŁKA, P., JABŁONOWSKA, A., MICKLITZ, H.W. e SARTOR, G., *Before machines consume the consumers. High-Level Takeaways from the ARTSY Project*, EUI Working papers, 2018

PALKA, P., Redefining «property» in the Digital Era. When online, do as the Romans did, 8, *EUI Working Paper Law*, 2016

PALMERINI, E., Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea, 6, *Responsabilità civile e previdenza*, 6, 2016

PALMIERI, N.F. III, Data Protection in an Increasingly Globalized World, 94, *Ind. L.J.*, 2019

PALMIERI, N.F. III, Who Should Regulate Data: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws, 11, *Hastings Sci. & Tech. L.J.*, 2020

PANETTA, R. (a cura di), Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018, Milano, Giuffré, 2019

PANETTA, R., *Il trasferimento all'estero dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019

PANETTA, R., *Privacy is not dead: it's hiring*!, in ID. (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato commentario al Regolamento UE n. 679/2016 e al D.Lgs. n. 101/2018*, Milano, Giuffré, 2019

PARDAU, S.L., EDWARDS, B., The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity, 12, *J. Of Bus. & Tech. L.*, 2017

PARDAU, S.L., 'The California Consumer Privacy Act: Towards a European-Style Privacy Regime in the United States', 23, *J Tech L & Pol'y*, 2018

PARDOLESI, A. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Vol. I, Milano, Giuffré, 2003

PARISI, A.G., *E-contract e privacy*, Torino, Giappichelli Editore, 2015

PASQUALE, F., Lecture, Response: Toward a Fourth Law of Robotics: Preserving Attribution, Responsibility, and Explainability in an Algorithmic Society, 78, *Ohio St. L.J.*, 2017

PASQUALE, F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015

PATTERSON, L.R., Free Speech, Copyright, and Fair Use, 40 *Vand. L. Rev.*, 1987

PATTI, S., *Consenso, sub art. 23*, in C.M. BIANCA, F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196*, t. I, Padova, Cedam, 2007

PATTI, S., Il consenso dell'interessato al trattamento dei dati personali, *Riv. dir. civ.*, 2, 1999

PEARL, J., MACKENZIE, D., *The Book of Why: The New Science of Cause and Effec*t, Basic Books, New York, 2018

PELINO, E., *I diritti dell'interessato*, in E. PELINO, L. BOLOGNINI, C. BISTOLFI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffré, Milano, 2016

PELLECCHIA, E., Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR, *NLCC*, 2, 2020

PELLECCHIA, E., *Privacy, decisioni automatizzate e algoritmi*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

PELLECCHIA, E., Profilazione e decisioni automatizzate al tempo della "Black Box Society": qualità dei dati e leggibilità dell'algoritmo nella cornice della "*responsible research and innovation*" in *Le Nuove leggi civili commentate*, 2018, 1209 ss

PERESIE, J.L., Toward a Coherent Test for Disparate Impact Discrimination, 84, *Indiana L.J.*, 2009

PERLINGERI, P., *L'informazione come bene giuridico*, in ID. (a cura di), *Il diritto dei contratti fra persona e mercato*, Napoli, Edizioni Scientifiche Italiane, 2003

PERLINGERI, P., L'informazione come bene giuridico, 2, *Rassegna di diritto civile*, 1990

PETRAGNANI, A.M., The Dormant Commerce Clause: On Its Last Leg, 57, *ALB. L. Rev.*, 1994

PHAN, K., FLO, T., PATEL, R., Recent Trends in the FTC's Data Security and Privacy Enforcement Actions, 19, *J. Internet L.*, 2016

PIERCE, R.J., Two Problems in Administrative Law: Political Polarity on the District of Columbia Circuit and Judicial Deterrence of Agency Rulemaking, *Duke L. J.*, 1988

PIERUCCI, A., *Elaborazione dei dati e profilazione delle persone*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

PINO, A., Contributo alla teoria giuridica dei beni, *Riv. Trim. dir. proc. civ.*, 1948

PIRAINO, F., Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato, 2, *Nuove leggi civ. comm.*, 2017

PISAPIA, A., *La tutela per il trattamento e la protezione dei dati personali*, Giappichelli Editore, Torino, 2018

PIZZETTI, F., (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli Editore, Torino, 2018

PIZZETTI, F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli Editore, Torino, 2016

PLOURDE-COLE, H. , Back to Katz: Reasonable Expectation of Privacy in the Facebook Age, 38, *Fordham Urb. L.J.*, 2, 2010

POLETTI, D., CAUSARANO, M.C., *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

POST, R., SHANOR, A., Adam Smith's First Amendment, 128, *Harv. L. Rev. F.*, 2015

POST, R., The Constitutional Concept of Public Discourse: Outrageous Opinion, Democratic Deliberation, and Hustler Magazine v. Falwell, 103, *Harv. L. Rev.*, 1990

PRAINSACK, B., *Data Donation: How to Resist the iLeviathan*, in J. KRUTZINNA, L. FLORIDI (a cura di), *The Ethics of Medical Data Donation*, Philosophical Studies Series, Vol. 137, Cham, Springer Open, 2019

PRIMUS, R.A., Equal Protection and Disparate Impact: Round Three, 117, *Harv. L. Rev.*, 2003

PRINS, C., *Property and Privacy: European Perspectives and the Commodification of our Identity*, in L. GUIBAULT, P.B. HUGENHOLTZ (a cura di), *The Future of the Public Domain. Identifying the Commons in Information Law*, The Hague, Kluwer Law International, 2006

PROSPERETTI, E., Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del Tar Lazio, in *Diritto dell'Informazione e dell'Informatica*, 2019, 979 ss.

PROSPERETTI, E., Accesso al software e al relativo algoritmo nei procedimenti amministrativi e giudiziali. Un'analisi a partire da due pronunce del TAR Lazio, *Diritto dell'Informazione e dell'Informatica*, 4, 2019

PROSSER, W.L., Privacy, 48, *California Law Review*, 3, 1960

PRUNTY, R. e SWARTZENDRUBER, A., *Social Media and the Fourth Amendment Privacy Protections* in N.S. LIND e E. RANKIN (a cura di), *Privacy in the Digital Age. 21st-Century Challenges to the Fourth Amendment*, Vol. 2, Santa Barbara (CA), ABC-CLIO LLC, 2015

PUGLIATTI, S., Beni (voce) (teoria generale), *Enc. dir*., Vol. V, Milano, Giuffré, 1959

PUGLIATTI, S., *Beni e cose in senso giuridico*, Milano, Giuffré, 1962

PUGLIATTI, S., Cosa (voce), *Enc. dir*., XI, Milano, Giuffré, 1962

PUGLIATTI, S., *La proprietà nel nuovo diritto*, II ed., Milano, Giuffré, 1964

PUGLIESE, G., Dalle «res ìncorporales» del diritto romano ai beni immateriali di alcuni sistemi giuridici odierni, *Rivista Trimestrale di Diritto e Procedura Civile*, 4, 1982

PUGLIESE, G., Diritti reali (voce), *Enc. dir*., XII, Milano, Giuffré, 1964

PURTOVA, N., The Illusion of Personal Data as No One's Property, 7, *Law, Innovation and Technology*, 1, 2015

RACHLINSKI, J.J., LYNN JOHNSON, S., WISTRICH, A.J., GUTHRIE, C., Does unconscious racial bias affect trial judges, 84, *Notre Dame L. Rev*., 2008

RADIN, M.J., A Comment on Information Propertization and Its Legal Milieu, 54, *Clev. St. L. Rev*., 2006

RADIN, M.J., *Contested Commodities. The Trouble with Trade in Sex, Children, Body Parts and Other Things*, Cambridg e (MA), Harvard University Press, 1996

RADIN, M.J., Property Evolving in Cyberspace, 15, *J.L. & Com*., 1996

RAI, A., Explainable AI. From Black Box to Glass Box, in Journal of the Academy of Marketing Science, 48, 2020, 137 ss

RAUL, A.C., FRONZONE, C.C. e TAPIA, S.S., *United States*, in A.C. RAUL (a cura di), *The Privacy, Data Protection and Cybersecurity Law Review*, VI ed., Law Business Research Lyd, Londra, 201

RAY, N.E., Let There Be False Light: Resisting the Growing Trend Towards an Important Tort, 84, *Minn. L. Rev*, 2000

RÉBÉ, N., *Artificial Intelligence: Robot Law, Policy and Ethics*, Leiden, Nijhoff, 2021

REDDIX-SMALLS, B., Credit Scoring and Trade Secrecy: An Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Finance Market, 12, *U.C. Davis Bus. L.J*., 2011

REICHMAN, J.H., FRANKLIN, J.A., Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information, 147, *U. Pa. L. Rev*., 1999

REIDENBERG, J.R., Setting Standards for Fair Information Practice in the U.S. Private Sector, 80, *Iowa L.Rev*., 1995

REINALTER, A., VALE, S., Cookie e consenso dell'utente, in Giur. It., 2020, 79 ss

REINALTER, A., VALE, S., Trattamento dei dati personali. Cookie e consenso dell'utente, in *Giur. It*., 2020, 1, 79 ss

RESCIGNO, P., *Disciplina dei beni e situazioni della persona*, in *Quaderni fiorentini per la storia del pensiero giuridico moderno*, V-VI.II, 1976/77

RESTA, G., Autonomia contrattuale e diritti della personalità nel diritto dell'UE (voce), *Dig. disc. priv*., Sez. civ., Torino, 2013

RESTA, G., *Dignità, persone e mercati*, Giappichelli Editore, Torino, 2014

RESTA, G., *Diritti esclusivi e nuovi beni immateriali*, Torino, Utet, 2010

RESTA, G., Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza, in *Politica del diritto*, n. 2, 2019, 199 ss.

RESTA, G., La disponibilità dei diritti fondamentali e i limiti della dignità (note a margine della carta dei diritti), *Rivista di diritto civile*, 2002

RESTA, G., La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE, in *Dir. Inf. e inform*., 2015

RESTA, G., *Nuovi beni immateriali e* numerus clausus *dei diritti esclusivi*, in ID. (a cura di), *Diritti esclusivi e nuovi beni immateriali*, Torino, Utet, 2011

RESTA, G., Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali, 7, *Riv. crit. dir. priv*., 2000

RESTA, G., V. ZENO-ZENCOVICH, Volontà e consenso nella fruizione dei servizi in rete, 2, *Rivista Trimestrale di Diritto e Procedura Civile*, 2018

RHOEN, M. e YI FENG, Q., Why the 'Computer says no': illustrating *Big Data*'s discrimination risk through complex systems science, 8, *International Data Privacy Law*, 2, 2018

RICCI, A., *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017

RICCI, A., Sulla "funzione sociale" del diritto alla protezione dei dati personali, 33, *Contr, e impr*esa, 2, 2017

RICCI, S., *Il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

RICCIO, G.M. E PEZZA, F., *Portabilità dei dati e interoperabilità*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

RICCIUTO, V., *Diritto dell'economia*, Giappichelli Editore, Torino, 2013

RICCIUTO, V., *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019

RICCIUTO, V., La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno, in *Diritto dell'Informazione e dell'Informatica*, 4, 2018, 709

RICCIUTO, V., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli Editore, Torino, 2019

RICH, M.L., Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, 164, *U. Pa. L. Rev*., 2016

RICHARDS, N., HARTZOG, W., The Pathologies of Digital Consent, 96 *Wash. U. L. Rev*., 2019

RICHARDS, N., *Intellectual Privacy: Rethinking Civil Liberties In The Digital Age*, Oxford, Oxford University Press, 2015

RICHARDS, N.M. e SOLOVE, D.J., Privacy's Other Path: Recovering the Law of Confidentiality, 96, *Geo. LJ*., 2007

RICHARDS, N.M. e SOLOVE, D.J., Prosser's Privacy Law: A Mixed Legacy, 98, *Calif. L. Rev*., 2010

RICHARDS, N.M., Intellectual Privacy, 87, *Text.L. Rev*., 2008

RICHARDS, N.M., The Limits of Tort Privacy, 9, *J. on Telecomm. & High Tech. L*., 2011

RICHARDS, N.M., W. HARTZOG, Taking Trust Seriously in Privacy Law, 19, *Stan. Tech. L. Rev*., 2016

RISCH, M., Why Do We Have Trade Secrets?, 11, *Marq. Intell. Prop. L. Rev*. 1, 2007

RITTER, J., MAYER, A., Regulating Data as Property. A New Construct for Moving Forward, 16, *Duke L & tech Rev*, 2018

ROBINSON, W.J., Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act, 98, *Georgetown Law Journal*, 4, 2010

RODOTÀ, S., *Tecnologie e diritti*, Bologna, Il Mulino, 1995

RODOTÀ, S., *Il diritto di avere diritti*, Roma, Laterza Editori, 2015

RODOTÀ, S., *Il mondo nella rete. Quali diritti, quali vincoli*, Editori Laterza, Roma, 2014

RODOTÀ, S., Tra diritti fondamentali ed elasticità della normativa. Il nuovo codice sulla privacy, *Europa e diritto privato*, 1, 2004

RODOTÀ, S., Tra diritto e società. Informazioni genetiche e tecniche di tutela, 18, *Riv. crit. Dir. priv*., 4, 2000

ROSSI DAL POZZO, F., La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal *Safe Harbour* al *Privacy Shield*), *Rivista di Diritto Internazionale*, 3, 2016

ROSSI, S., Consenso informato (voce), *Digesto*, sez. civ., VII, Torino, Utet, 2012

ROSTOW, T., What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers, 34, *Yale J. On Reg*., 2017

ROTHMAN, J., The Inalienable Right of Publicity, 101, *Georgetown Law Journal*, 2012

RUBINSTEIN, I.S., LEE, R.D., SCHWARTZ, P.M., Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches, 75 *U. Chi. L. Rev*., 2008

RYAN CALO, M., Against Notice Skepticism in Privacy (and Elsewhere), 87, *Notre Dame L. Rev*., 2012

S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006

SALES, L., Algorithms, Artificial Intelligence and the Law, *Judicial Review*, 25, 2020

SALUZZO, S., Cross Border Data Flows and International Trade Law the Relationship Between EU Data Protection Law and the GATS, *Diritto del Commercio Internazionale*, 4, 2017

SALVADORI, I., Agenti artificiali, opacità tecnologica e distribuzione della responsabilità penale, *Rivista italiana di diritto e procedura penale*, 1, 2021, 83 ss

SAMAHA, J. *Criminal Procedure*, X ed., Belmont (CA), Wadsworth, 2018

SAMUEL, I., The New Writs of Assistance, 86, *Fordham L. Rev*., 2018

SAMUELSON, P., Privacy as Intellectual Property, 52, *Stan. L. Rev*., 2000

SARDINI, A., La "*Product Liability*" e il commercio elettronico, Il diritto dell'informazione e dell'informatica, 1, 2021, 81 ss

SARGENT, S., Fight or Comply: the Federal Trade Commission's Power to Hold Companies Liable for Data Security Breaches, 41, *J. Corp. L*., 2015

SARTOR, G., *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano, Giuffré Editore, 1990, 28 ss

SARZANA DI S. IPPOLITO NICOTRA, F. M., *Diritto della* blockchain*, intelligenza artificiale e IoT*, Ipsoa, Milano, 2018

SATTA, S., Cose e beni nell'esecuzione forzata, 9-10, *Rivista del diritto commerciale*, 1964

SCHAFF, S., La nozione di informazione e la sua rilevanza giuridica, 2, *Diritto dell'informazione e dell'informatica*, 1987

SCHAUESR, F., Internet Privacy and the Public-Private Distinction, 38, Jurimetrics, 4, 1998

SCHERMER, B., *Risks of Profiling and the Limits of Data Protection Law*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*, Springer, Berlino, 2013

SCHERMER, B.W., The Limits of Privacy in Automated Profiling and Data Mining, 27, *Computer Law & Security Review*, 1, 2011

SCHNEIDER, G.M., GERSTING, J.L., *Informatica*, RN, Maggioli Editore, 2013

SCHNEIER, B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, I ed., New York, W.W. Norton & Company, 2015

SCHOLZ, L.H., Privacy as Quasi-Property, 101, *Iowa Law Review*, 2016

SCHRIVER, R.R., You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission, 70, *Fordham L. Rev.*, 2002

SCHUCK, P.H., Rethinking Informed Consent, 103, *Yale L.J.*, 1994

SCHULTZ, D., e VILE, J.R., *The Encyclopedia of Civil Liberties in America*, New York, Routledge, 2015

SCHWARTZ, P., Property, Privacy and Personal Data, 117, *Harv. L. Rev.*, 2004

SCHWARTZ, P.M., Global Data Privacy: The EU Way, 94, *N.Y.U. L. REV.*, 2019

SCHWARTZ, P.M., Internet Privacy and the State, 32, *Connecticut Law Review*, 3, 2000

SCHWARTZ, P.M., PEIFER, K.N., Transatlantic Data Privacy Law, 106, *Geo. L.J.*, 2017

SCHWARTZ, P.M., Privacy and Democracy in Cyberspace, 52, *Vand. L. Rev.*, 1999

SCHWARTZ, P.M., SOLOVE, D. J., Reconciling Personal Information in the United States and European Union, 102, *California Law Review*, 4, 2014

SCHWARTZ, P.M., SOLOVE, D.J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86, *N.Y.U. L. Rev.*, 2011

SCHWARTZ, P.M., The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures, 126, *Harv. L. Rev.*, 2013

SCIALOJA, V., *Teoria della proprietà nel diritto romano*, Vol. I, Roma, Attilo Sampaolesi, 1928

SCOTT, M.D., *Scott on Multimedia Law*, IV ed., Wolters Kluwer, New York, 2019

SCOTT, M.D., The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?, 60, *Admin. L. Rev.*, 2008

SCOZZAFAVA, O.T., *I beni e le forme giuridiche di appartenenza*, Vol. 32, Milano, Giuffrè, 1982

SCUDIERO, L., *Il consenso come condizione di liceità*, in G. CASSANO, V. COLAROCCO, G. BATTISTA GALLUS, F.P. MICOZZI (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D. lgs. 10 agosto 2018, n. 101*, Milano, Giuffré, 2018

SEARLE, J.R., Minds, Brains and Science, 3, *Behavioral and Brain Sciences*, 1980

SELBST, A.D., e BAROCAS, S., The Intuitive Appeal of Explainable Machines, 87, *Fordham L. Rev*, 3, 2018

SELBST, A.D., e POWLES, J., Meaningful Information and the Right to Explanation, 7, *International Data Privacy Law*, 4, 2017

SENEVIRATNE, S. *et al*., Predicting User Traits from a Snapshot of Apps Installed on a Smartphone, 18, *Mobile Computing and Communications Review*, 1, 2015

SENIGAGLIA, R., La dimensione patrimoniale del diritto alla protezione dei dati personali, in *Contratto e Impresa*, 2020, 760 ss

SERWIN, A., The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices, 48, *San Diego L. Rev.*, 2011

SICA, S., Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica, *Riv. dir. civ*., 2001

SICA, S., V. D'ANTONIO, I *Safe Harbour Privacy Principles*: Genesi, Contenuti, Criticità, *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015

SICA, S., V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei* Safe Harbour Privacy Principles, in. V. ZENO ZENCOVICH e G. RESTA (a cura di), *La protezione transnazionale dei dati personali: dai* Safe Harbour Principles *al "*Privacy Shield*"*, Roma Tre E-Press, Roma, 2016

SIMITIS, S., Il contesto giuridico e politico della tutela della privacy, *Riv. crit. dir. priv*., 4, 1997

SIMONCINI, M., Lo «stato digitale». L'agire provvedimentale dell'amministrazione e le sfide dell'innovazione tecnologica, *Rivista Trimestrale di Diritto Pubblico*, 2, 2021

SLOANE, J.N., Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation', 12, *J. Marshall L.J*., 23, 2019

SMUHA, N.A., From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence, 13, *Law, Innovation and Technology*, 2021

SOLINAS, C., Trattamento dei dati personali e pratiche commerciali scorrette, in *Giur. It.*, 2, 320 ss

SOLOVE, D., e SCHWARTZ, P.M., *Information Privacy Law*, VI ed., Aspen Casebook Series, Wolters Kluwer, New York, 2018

SOLOVE, D.J. e HARTZOG, W., The FTC and the New Common Law of Privacy, 114, *Colum. L. Rev*., 2014

SOLOVE, D.J., Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75, *S. Cal. L. Rev*., 2002

SOLOVE, D.J., I've Got Nothing to Hide' and Other Misunderstandings of Privacy, 44, *San Diego L. Rev*., 2007

SOLOVE, D.J., KEATS CITRON, D., Risk and Anxiety: A Theory of Data-Breach Harms, 96, *Tex. L. Rev*., 2018

SOLOVE, D.J., M. ROTENBERG, P. M. SCHWARTZ, *Privacy, Information, and Technology*, New York, Aspen Publishers, 2006

SOLOVE, D.J., *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, New Haven, 2011

SOLOVE, D.J., P.M. SCHWARTZ, ALI Data Privacy: Overview and Black Letter Text, 68, *UCLA Law Review*, 2020

SOLOVE, D.J., Privacy Self-Management and the Consent Dilemma, 126, *Harv. L. Rev*., 2013

SOLOVE, D.J., *The Digital Person: Technology and Privacy in the Information Age*, New York, NYU Press, 2004

SOLOVE, D.J., *Understanding Privacy*, Harvard University Press, Cambridge (MA), 2008

SOLUM, L.B., Legal Personhood for Artificial Intelligences, 70, *N.C. L. Rev*., 1992

SONG, Q., JIN, H., HUANG, X., HU, X., Multi-Label Adversarial Perturbations, *arXiv:1901.00546*, 2019

SPANGARO, A., *L'ambito di riferimento materiale del nuovo regolamento*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli, Bologna, Vol. 25, 2017

SPIEKERMANN, S., *Ethical IT Innovation. A Value-Based System Design Approach*, Taylor & Francis Group, Boca Raton, 2016

SPINELLI, C.J., Far From Fair, Farther From Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking, 6, *Am. Univ. Leg. And Policy Brief*, 2014

SPIVAK, R., Too Big a Fish in the Digital Pond: The California Consumer Privacy Act and the Dormant Commerce Clause, 88, *U. Cin. L. Rev.*, 2020

SPLICHAL, S.L., The evolution of computer/privacy concerns: Access to government information held in the balance, 1, *Communication Law and Policy*, 2, 1996

STANZIONE, A.G., Il regolamento europeo sulla privacy: origini e ambito di applicazione, *Europa e Diritto Privato*, 4, 2016

STAZI, A., CORRADO, F., Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica, *Diritto dell'Informazione e dell'Informatic*a, 2, 2019

STEGMAIER, G.M., BARTNICK, W., Another Round in the Chamber: FTC Data Security Requirements and the Fair Notice Doctrine, 5, *J. Internet L*., 2013

STEGMAIER, G.M., BARTNICK, W., Psychics, Russian Roulette, and Data Security: The FTC's Hidden Data Security Requirements, 20 *Geo. Mason L. Rev*., 2013

STOLFI, N., *Il diritto di autore*, Milano, Società Editrice Libraria, 1932

STONE, C.D., *Should Trees Have Standing? Law, Morality, and the Environment*, III ed., Oxford University Press, Oxford, 2010

STRAUSS, P., RAKOFF, T., FARINA, C. e METZGER, G., *Gellhorn and Byse's Administrative Law: Cases and Comments*, XI ed., Foundation Press, 2011

STRINATI, C., Algoritmi e decisioni amministrative, *Il Foro Amministrativo*, 7, 2020

STUNTZ, W., *Search and Seizure*, in J. DRESSLER (a cura di), *Encyclopedia of Crime & Justice*, II ed., New York, Macmillan Reference USA, 2002

SUNSTEIN, C.R., *Free Markets and Social Justice*, Oxford, Oxford University Press, 1997

SWIRE, P. e KENNEDY-MAYO, D., How Both the EU and the U.S. Are "Stricter" than Each Other for the Privacy of Government Requests for Information, 55, *EMORY L.J.*, 2017

SWIRE, P.P. e AHMAD, K., *Foundations of Information Privacy And Data Protection*, International Association of Privacy Professionals, Portsmouth, 2012

SWIRE, P.P., LITAN, R.E., *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Brookings Institution Press, 1998

TABARRINI, C., Comprendere la "Big Mind": il GDPR sana il divario di intelligibilità uomo-macchina?, 2, *Diritto dell'Informazione dell'Informatica*, 2019

TAYLOR, L., FLORIDI, L., VAN DER SLOOT, B., *Introduction: A New Perspective on Privacy*, in ID. (a cura di), *Group Privacy*. *New Challenges of Data Technologies*, Philosophical Studies Series, Vol. 126, Springer, Berlino, 2017

TAYLOR, R., No Privacy Without Transparency, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura si) *Data Protection and Privacy: The Age of Intelligent Machines*, Hart Publishing, Oxford, 2017

TAYLOR, W.F., Meeting the Equal Credit Opportunity Act's Specificity Requirement: Judgmental and Statistical Scoring Systems, 29 *Buff. L. Rev.*, 1980

TEN, C.L., Mill's *On Liberty.A Critical Guide*, Cambridge, Cambridge University Press, 2009

TENE, O. e POLONETSKY, J., Taming the Golem: Challenges of ethical algorithmic decision-making, 19, *NCJL & Tech.*, 2017

TENE, O., POLONETSKY, J., *Big Data* for All: Privacy and User Control in the Age of Analytics, 11, *Nw.K. Tech. & Intell. Prop.*, 2013

TEROLLI, E., Privacy e protezione dei dati personali IE vs USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II", *Diritto dell'informazione e dell'informatica*, 1, 2021, 49 ss

TEUBNER, G., *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Edizioni Scientifiche Italiane, Napoli, 2019

THOBANI, S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018

THOBANI, S., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Ledizioni, Milano, 2018, 46

THOBANI, S., Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente, in *MediaLaws - Rivista di diritto dei media*, 3, 2019, 131-147

THOBANI, S., Protezione dei dati personali - operazioni di *tying* e libertà del consenso, 3, *Giur. It.*, 2019

TORONTO, U. L.J., Law as Information in the Era of Data-Driven Agency, 79, *Mod. L. Rev.*, 2016

TOSI, E., Illecito trattamento dei dati personali, responsabilizzazione, responsabilità oggettiva e danno nel GDPR: funzione deterrente-sanzionatoria e rinascita del danno morale soggettivo, *Contratto e impresa*, 3, 2020, 1115 ss

TOSI, E., La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR) (prima parte)., *Studium Iuris*, 7-8, 2020

TOSI, E., La responsabilità civile per trattamento illecito dei dati personali alla luce del General Data Protection Regulation (GDPR)(seconda parte), *Studium Iuris*, 9, 2020

TOSI, E., *Privacy digitale, persona e mercato: tutela della riservatezza e protezione dei dati personali alla luce del GDPR e del nuovo codice privacy* , in ID. (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffré, 2019

TOSI, E., Trattamento illecito dei dati personali, responsabilità oggettiva e danno non patrimoniale alla luce dell'art. 82 del GDPR UE, *Danno e responsabilità*, 4, 2020

TOWNSEND, D., Who Should Define Injuries for Article III Standing?, 68, *Stan. L. Rev. Online*, 2015

TURING, A.M., Computing Machinery and Intelligence, 49, *Mind*, 1950

tutela del consumatore, *Giurisprudenza Commerciale*, 4, 2020

UBERTAZZI, L.C. (a cura di), *La proprietà intellettuale*, Giappichelli, Torino, 2011

URSUL, M., The States' Role in Data Privacy: California Consumer Privacy Act versus Dormant Commerce Clause, 52, *Suffolk U. L. Rev.*, 2019

VALLE, L., GRECO, L., Transnazionalità del trattamento dei dati personali e tutela degli interessati, tra strumenti di diritto internazionale privato e la prospettiva di principi di diritto privato di formazione internazionale, *Diritto dell'Informazione e dell'Informatica*, 2, 2017

VAN DIJCK, J. , Datafication, dataism and dataveillance: *Big Data* between scientific paradigm and ideology, 12, *Surveillance & Society*, 2, 2014

VAN LOO, R., Making Innovation More Competitive: The Case of Fintech, 6, *UCLA L. Rev.*, 2018

VANNI, D., Protezione dei dati personali (voce), *Digesto*, 2013

VAUGHAN, L., *Mapping Society. The Spatial Dimensions of Social Cartography*, UCL Press, 2018

VEDDER, A.H., *Privatization, information technology and privacy: Reconsidering the social responsibilities of private organizations*, in G. MOORE (a cura di), *Business ethics: Principles and practice*, Warwick, Business Education Publishers, 1997

VERSACI, G., La contrattualizzazione dei dati personali dei consumatori, Napoli, ESI, 2020

VICTOR, J.M., The Eu General Data Protection regulation: Toward a Property Regime for Protecting Data Privacy, *Yale Law Journal*, 2013

VIOLA, L., L'Intelligenza Artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte, 2, *Foro Amministrativo*, 9, 2018

VIVIENNE, S. e THORNTON, P., *Beyond Implicit Political Dichotomies and Linear Models of Change in China*, in ID. (a cura di), *To Govern China: Evolving Practices of Power*, Cambridge, Cambridge University Press, 2017

VOLOKH, E., Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You, 52, *Stan. L. Rev*., 2000

WACHTER, S., MITTELSTADT, B. e FLORIDI, L., Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7, *International Data Privacy Law*, 2, 2017

WACHTER, S., MITTELSTADT, B., RUSSELL, C., Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, 31, *Harvard Journal of Law & Technology*, 2, 2018

WALDMAN, A.E., Designing Without Privacy, 55, *Houston L.Rev*., 2018

WEINSTOCK NETANEL, N., Cyberspace Self-Governance: 4 Skeptical View from Liberal Democratic Theory, 88 *Cal. L. Rev*., 2000

WESLEY CAMPBELL, E., But It's Written in Pen: The Constitutionality of California's Internet Eraser Law, 48, *Colum. J.L. & Soc. Probs*, 2015

WESTIN, A., *Privacy and Freedom*, II ed., New York, Ig Publishing, 2015

WILLIAMS, R.C., Due Process, Class Action Opt Outs, and the Right Not to Sue, 115, *COLUM. L. Rev*., 2015

WISCHMEYER, T., *Artificial Intelligence and Transparency: Opening the Black Box*, in T. WISCHMEYER, T. RADEMACHER (a cura di), *Regulating Artificial Intelligenc*e, Springer, Cham, 2020

WOLF, H.G., *Drones. Safety Risk Management for the Next Evolution of Flight*, New York, Routledge, 2017

XU, A., Chinese Judicial Justice on the Cloud: A Future Call or a Pandora's Box? An Analysis of the 'Intelligent Court System' of China, 26, *Information & Communications Technology Law*, 1, 59, 2017

ZANOVELLO, F., Consenso libero e specifico alle *e-mail* promozionali, 12, *NGCC*, 2018

ZARSKY, T., The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making, 41, *Science, Technology, & Human Values*, 2016

ZARSKY, T., *Transparency in Data Mining: From Theory to Practice*, in B. CUSTERS, T. CALDERS, B. SCHERMER, e T. ZARSKY (a cura di), *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*, Springer, Berlino, 2013

ZARSKY, T.Z. Transparent Predictions, *U. Ill. L. Rev*., 2013

ZARSKY, T.Z., "Mine your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion, 5, *Yale Journal of Law and Technology*, 1, 2003

ZARSKY, T.Z., Governmental Data Mining and Its Alternatives, 116, *Penn St. L. Rev*., 2011

ZENO ZENCOVICH, V. *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, Giuffré, 1999

ZENO ZENCOVICH, V., Dati, grandi dati, dati granulari e la nuova epistemologia del giurista, *Rivista di diritto dei media*, 2, 2018

ZENO ZENCOVICH, V., I negozi sugli attributi della personalità, *Diritto dell'informazione e dell'informatica*, 3, 1993

ZENO ZENCOVICH, V., Informazione (profili civilistici) (voce), *Digesto Disc. Priv.*, Sez. civ., Vol. IX, Torino, 1993

ZENO ZENCOVICH, V., Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in *Dir. inf. E inform*., 2015

ZENO ZENCOVICH, V., Personalità (diritti della) (voce), *Dig. disc. priv*., Sez. civ., I, XIII, Torino, 1995

ZENO ZENCOVICH, V., Sull'informazione come "bene" (e sul metodo del dibattito giuridico), 17, *Riv. crit. dir. priv*., 3, 1999

ZENO ZENCOVICH, V., Ten Legal Perspectives on the "Big Data Revolution", 1, *Concorrenza e mercato*, 29, 2016

ZENO-ZENCOVICH, V., Do "Data Markets" Exist?, in *MediaLaws*, 2, 2019, 23

ZIFF, D.J., Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant, 105 *Colum. L. Rev*., 2005

ZIMMERMAN, D.L., False Light Invasion of Privacy: The Light That Failed, 64, *N.Y.U. L. rev*., 1989

ZIMMERMAN, D.L., Livinig Without Copyright in a Digital World, 70, *Albany Law Review*, 2007

ZITTRAIN, J., How to Exercise the Power You Didn't Ask For, *Harv. Bus. Rev*., 2018

ZOPPINI, A., Le «nuove proprietà» nella trasmissione ereditaria della ricchezza (note a margine dellateoria dei beni), 2, *Riv. Dir. Civ*., 2000

ZORZI GALGANO, N., *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*, Cedam, 2019

ZUBOFF, S., *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019

Università
Ca'Foscari
Venezia

DEPOSITO ELETTRONICO DELLA TESI DI DOTTORATO

DICHIARAZIONE SOSTITUTIVA DELL'ATTO DI NOTORIETA'

(Art. 47 D.P.R. 445 del 28/12/2000 e relative modifiche)

Io sottoscritto ... CAMILLA ... TABARRINI .....

nat a a ... ROMA ..... (prov. RM.) il ... 11/06/1993 ...

residente a ... PALOMBARA S. ... in STRADA DEL LAGHETTO ..... n. 98 ...

Matricola (se posseduta) 956437 ..... Autore della tesi di dottorato dal titolo:

LA TRASPARENZA ALGORITMICA NEL TRATTAMENTO DEI DATI PERSONALI. PROSPETTIVE EUROUNITARIE E STATUNITENSI .....

.....

Dottorato di ricerca in ... DIRITTO, MERCATO E PERSONA .....

(in cotutela con ..... /.....)

Ciclo ... 34° .....

Anno di conseguimento del titolo ... 2022 .....

DICHIARO

di essere a conoscenza:

1) del fatto che in caso di dichiarazioni mendaci, oltre alle sanzioni previste dal codice penale e dalle Leggi speciali per l'ipotesi di falsità in atti ed uso di atti falsi, decado fin dall'inizio e senza necessità di nessuna formalità dai benefici conseguenti al provvedimento emanato sulla base di tali dichiarazioni;

2) dell'obbligo per l'Università di provvedere, per via telematica, al deposito di legge delle tesi di dottorato presso le Biblioteche Nazionali Centrali di Roma e di Firenze al fine di assicurarne la conservazione e la consultabilità da parte di terzi;

3) che l'Università si riserva i diritti di riproduzione per scopi didattici, con citazione della fonte;

4) del fatto che il testo integrale della tesi di dottorato di cui alla presente dichiarazione viene archiviato e reso consultabile via Internet attraverso l'Archivio Istituzionale ad Accesso Aperto dell'Università Ca' Foscari, oltre che attraverso i cataloghi delle Biblioteche Nazionali Centrali di Roma e Firenze;

5) del fatto che, ai sensi e per gli effetti di cui al D.Lgs. n. 196/2003, i dati personali raccolti saranno trattati, anche con strumenti informatici, esclusivamente nell'ambito del procedimento per il quale la presentazione viene resa;

6) del fatto che la copia della tesi in formato elettronico depositato nell'Archivio Istituzionale ad Accesso Aperto è del tutto corrispondente alla tesi in formato cartaceo, controfirmata dal tutor, consegnata presso la segreteria didattica del dipartimento di riferimento del corso di dottorato ai fini del deposito presso l'Archivio di Ateneo, e che di conseguenza va esclusa qualsiasi responsabilità dell'Ateneo stesso per quanto riguarda eventuali errori, imprecisioni o omissioni nei contenuti della tesi;

7) del fatto che la copia consegnata in formato cartaceo, controfirmata dal tutor, depositata nell'Archivio di Ateneo, è l'unica alla quale farà riferimento l'Università per rilasciare, a richiesta, la dichiarazione di conformità di eventuali copie;

Data 3/11/21 **Firma** Camilla Tabarrini

NON AUTORIZZO

l'Università a riprodurre ai fini dell'immissione in rete e a comunicare al pubblico tramite servizio on line entro l'Archivio Istituzionale ad Accesso Aperto la tesi depositata per un periodo di 12 (dodici) mesi a partire dalla data di conseguimento del titolo di dottore di ricerca.

DICHIARO

1) che la tesi, in quanto caratterizzata da vincoli di segretezza, non dovrà essere consultabile on line da terzi per un periodo di 12 (dodici) mesi a partire dalla data di conseguimento del titolo di dottore di ricerca;
2) di essere a conoscenza del fatto che la versione elettronica della tesi dovrà altresì essere depositata a cura dell'Ateneo presso le Biblioteche Nazionali Centrali di Roma e Firenze dove sarà comunque consultabile su PC privi di periferiche; la tesi sarà inoltre consultabile in formato cartaceo presso l'Archivio Tesi di Ateneo;
3) di essere a conoscenza che allo scadere del dodicesimo mese a partire dalla data di conseguimento del titolo di dottore di ricerca la tesi sarà immessa in rete e comunicata al pubblico tramite servizio on line entro l'Archivio Istituzionale ad Accesso Aperto.

Specificare la motivazione:
☑ motivi di segretezza e/o di proprietà dei risultati e/o informazioni sensibili dell'Università Ca' Foscari di Venezia.
□ motivi di segretezza e/o di proprietà dei risultati e informazioni di enti esterni o aziende private che hanno partecipato alla realizzazione del lavoro di ricerca relativo alla tesi di dottorato.
□ dichiaro che la tesi di dottorato presenta elementi di innovazione per i quali è già stata attivata / si intende attivare la seguente procedura di tutela:

.....;

□ Altro (specificare):

.....

.....

.....

A tal fine:
- dichiaro di aver consegnato la copia integrale della tesi in formato elettronico tramite auto-archiviazione (upload) nel sito dell'Università; la tesi in formato elettronico sarà caricata automaticamente nell'Archivio Istituzionale ad Accesso Aperto dell'Università Ca' Foscari, dove rimarrà non accessibile fino allo scadere dell'embargo, e verrà consegnata mediante procedura telematica per il deposito legale presso la Biblioteca Nazionale Centrale di Firenze;
- consegno la copia integrale della tesi in formato cartaceo presso la segreteria didattica del dipartimento di riferimento del corso di dottorato ai fini del deposito presso l'Archivio di Ateneo.

Data 3/11/21 **Firma** Paulla Stanzi

La presente dichiarazione è sottoscritta dall'interessato in presenza del dipendente addetto, ovvero sottoscritta e inviata, unitamente a copia fotostatica non autenticata di un documento di identità del dichiarante, all'ufficio competente via fax, ovvero tramite un incaricato, oppure a mezzo posta.

Firma del dipendente addetto .....

Ai sensi dell'art. 13 del D.Lgs. n. 196/03 si informa che il titolare del trattamento dei dati forniti è l'Università Ca' Foscari - Venezia.
I dati sono acquisiti e trattati esclusivamente per l'espletamento delle finalità istituzionali d'Ateneo; l'eventuale rifiuto di fornire i propri dati personali potrebbe comportare il mancato espletamento degli adempimenti necessari e delle procedure amministrative di gestione delle carriere studenti. Sono comunque riconosciuti i diritti di cui all'art. 7 D. Lgs. n. 196/03.

Estratto per riassunto della tesi di dottorato

Studente: Camilla Tabarrini

Matricola: 956437

Dottorato: Diritto, Mercato e Persona

Ciclo: 34°

Titolo della tesi: La trasparenza algoritmica nel trattamento dei dati personali. Prospettive eurounitarie e statunitensi

Abstract:

Oggetto del lavoro di ricerca è la disciplina del trattamento automatizzato di dati personali a fini decisionali. L'analisi si articola in tre livelli. Il primo consiste nell'inquadramento dogmatico dei diritti che il titolare può esercitare sul dato personale e sulle informazioni dallo stesso inferite (cc.dd. metadati), al fine di porre le basi ermeneutiche del bilanciamento tra diritti di privativa industriale sui metadati utilizzati a fini decisionali e il diritto degli interessati ad avere una spiegazione significativa delle determinazioni automatizzate per tal via assunte nei propri confronti *ex* art. 22 GDPR. È proprio alla ricostruzione normativa e operativa del contenuto di tale spiegazione che verrà quindi dedicato il secondo livello dello studio, mettendo in luce i limiti giuridici e tecnologici delle varie proposte dottrinali. Individuato così un modello di spiegazione *ante* e *post* reclamo, si concluderà offrendo, *de iure condito*, una panoramica casistica delle soluzioni legislative adottate negli USA in punto di processi decisionali automatizzati e trasparenza e, *de iure condendo*, spunti di riflessione prognostici sulle linee evolutive della *data privacy* statunitense.

The research focuses on the legal discipline of automated data processing for decision-making purposes. The analysis is threefold. Firstly, it deals with the legal nature of the rights data controller can exercise over personal data and inferred metadata. The objective is to shed a preliminary interpretative light over the conflicting rights underpinning the right to an explanation pursuant to article 22 GDPR: IP rights over metadata and transparency rights over the logic followed to take AI-based decisions. This intelligibility threshold and its regulatory framework under the GDPR is precisely the focus of the second chapter, which is aimed at developing an operative model for meaningful pre-claim and post-claim explanations. Lastly, the third chapter concludes by presenting a case-based overview of the US regulatory approach towards algorithmic decision-making and transparency as well as few legislative hints of possible data privacy regulatory developments.

Firma dello studente