X CONVEGNO ANNUALE DELL'ASSOCIAZIONE ITALIANA DEI PROFESSORI UNIVERSITARI
DI DIRITTO COMMERCIALE "ORIZZONTI DEL DIRITTO COMMERCIALE"
"*L'EVOLUZIONE TECNOLOGICA E IL DIRITTO COMMERCIALE*"
Roma, 22-23 febbraio 2019

GIULIA SCHNEIDER

Due facce dello stesso algoritmo: "verificabilità" della processazione automatica dei dati personali e tutela dei segreti commerciali nel quadro europeo

SOMMARIO: 1. Introduzione – 2. Il principio di trasparenza nella sistematica del Regolamento Generale Dati Personali- 2.1 La prospettiva *ex ante*: trasparenza e progettazione algoritmica- 2.2 La prospettiva *ex post*: trasparenza e responsabilità- 3. Le disposizioni sulla trasparenza nel Regolamento Generale Dati Personali- 3.1 Il diritto alla "spiegazione algoritmica": il dibattito sulla natura sostanziale e funzionale-3.2. Le informazioni sulla logica utilizzata dal trattamento automatizzato: dalla spiegazione alla verificabilità algoritmica- 4. L'altra faccia dell'algoritmo: la tutela del segreto commerciale- 4.2 Il paradigma del segreto sulle informazioni relative al trattamento automatizzato: implicazioni *intra*- ed *extra*-sistemiche 5. Il bilanciamento tra diritti di verificabilità e diritto alla segretezza algoritmica: le soluzioni della giurisprudenza- 5.1 La soluzione interpretativa: verso una ricomposizione del mosaico normativo- 5.2. La soluzione operativa: la tutela "modulata" del segreto commerciale- 6. Conclusioni

1. *Introduzione*

L'intelligenza artificiale quale nuovo strumento di erogazione di servizi digitali è alla base di profondi mutamenti strutturali del tessuto economico contemporaneo. Il crescente impiego di strumenti di processazione algoritmica da parte delle imprese attive nel mercato digitale sta trasformando gli scenari di sfruttamento dei dati personali a scopo commerciale: il trattamento di dati personali su larga scala mediante algoritmi consente la massiccia aggregazione dei dati personali disseminati online; l'analisi degli stessi per la identificazione di correlazioni; e sulla

scorta di queste, la creazione di modelli che da ultimo orientano in via "automatizzata" le operazioni commerciali delle imprese digitali[1].
La natura "generativa" degli algoritmi ha decretato il successo dirompente di tale tecnologia, divenuta primaria fonte di previsione e valutazione dei comportamenti degli utenti e dunque norma comportamentale delle c.d. piattaforme digitali[2].
Le tecniche analitiche basate su algoritmi hanno dato adito a nuovi fenomeni di profilazione collettiva, consistenti in operazioni di vera e propria *clusterizzazione* degli utenti, raggruppati secondo caratteristiche comuni e resi così destinatari di trattamenti commerciali omogenei[3].
In questo contesto, le tecniche di processazione algoritmica appaiono contraddistinte da una duplice portata economica e giuridica: *a monte* quale *asset* immateriale dotato di valenza strategico-competitiva per le società processanti; *a valle* quale mezzo altamente invasivo della sfera privata degli utenti. Questi ultimi forniscono l'input primario delle infrastrutture processanti attraverso la diffusione online di dati personali per subire poi gli effetti delle conseguenti decisioni automatizzate.
Dal punto di vista normativo, ciò fa sì che le tecnologie di processazione algoritmica siano al contempo oggetto della disciplina di proprietà intellettuale, in quanto porzione (sempre più considerevole) del patrimonio immateriale delle imprese che si avvalgono di tali nuove tecnologie, e della disciplina in materia di protezione di dati personali, in quanto strumento di trattamento dei medesimi dati a scopi decisionali. Ne consegue una parziale sovrapposizione di due distinte discipline, l'una mirante alla promozione

---

[1] Cfr. M. MAGGIOLINO, *I Big data e il diritto antitrust*, Milano, Egea, 2018, 5 ss..
[2] R. GELLERT, *Understanding Data Protection as Risk Regulation*, in *Journal of Internet Law*, 2015, 6 ss.; K. CRAWFORD- J. SCHULTZ, *Big Data and Due Process: Towards a Framework to Redress Predictive Privacy Harms,* in *Boston College Law Review*, 2014, 55, 93 ss..
[3] È difatti noto come le operazioni di processazione algoritmica di dati siano condotte sulla base di categorie predeterminate di soggetti che costituiscono il modello che orienta i processi decisionali aziendali dispiegantisi sempre maggiormente lungo direttrici di stigmatizzazione e discriminazione commerciale. Si tratta del fenomeno della c.d. "clusterizzazione", altresì noti come "profili di gruppo". Cfr. ampiamente, L. TAYLOR-L. FLORIDI-B. VAN DER SLOOT, *Group Privacy-New Challenges of Data Technologies*, Springer, 2016, *passim;* B. VAN DER SLOOT, *The Individual In the Big Data Era: Moving towards an agent-based Privacy Paradigm,* cit., 193, ove l'A. afferma come "in the current technological environment, however, the direct connection of data to an individual is becoming less evident. Data increasingly have a circular life cycle: they may begin as individual data, then be linked to other data so they become sensitive data, then be aggregated and anonymized in a group profile and then a specific individual may finally be linked to the group profile".

del progresso tecnologico attraverso la predisposizione di strumenti di tutela del frutto degli investimenti delle imprese e l'altra volta alla creazione di un apparato protettivo dei soggetti interessati dal trattamento di dati personali.

Come questo contributo intende dimostrare, in relazione alla tecnologia degli algoritmi il conflitto tra esigenze di protezione di proprietà intellettuale e di protezione dei dati personali assume caratteri nuovi rispetto al passato. Sul piano europeo, entrambe le discipline hanno subito notevoli mutamenti per effetto, rispettivamente, della Direttiva UE 2016/943[4] in materia di tutela del segreto commerciale e del Regolamento UE 679/2016[5] che predispone una disciplina radicalmente nuova in materia di protezione di dati personali: entrambi i corpi normativi costituiscono una pronta risposta regolatoria al fenomeno della "algoritmizzazione" del settore digitale.

Dopo aver definito i caratteri della trasparenza algoritmica demandata dal Regolamento dati personali, il saggio si propone di indagare la rilevanza della tutela del segreto commerciale rispetto ai trattamenti automatizzati di dati personali, suggerendo una lettura trasversale della disciplina europea in materia di segreti commerciali. In conclusione intende quindi dimostrare come solo una "tutela modulata" del segreto commerciale sia idonea a garantire una piena tutela del diritto fondamentale alla *privacy* nelle sue nuove vesti di diritto alla verificabilità del trattamento automatizzato.

2. Il principio di trasparenza nella sistematica del Regolamento Generale Dati Personali

Secondo la ricostruzione di una parte di dottrina, la disciplina in materia dei dati personali ha storicamente assunto una triplice funzione: quella di strumento di controllo del dato personale, della sua integrità e infine

[4] 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, OJ L 157, 15 giugno 2016, 1–18.

[5] Regolamento UE 2016/679 del Paramento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati personali), OJ L 119, 4 Maggio 2016, 1–88. Di seguito RGDP.

dell'accesso a questo[6]. La recente riforma europea in materia di dati personali sembra essere rimasta aderente, in una soluzione di continuità rispetto al passato, ai due paradigmi del controllo e dell'integrità dei dati personali processati, come compiutamente delineati nella precedente direttiva[7] e nelle successive trasposizioni nazionali.

La portata innovativa del Regolamento in materia di dati personali 2016/679 sembra diversamente risiedere nella nuova preminenza conferita dallo stesso al profilo dell'accesso all'informazione. Le molteplici disposizioni ivi contenute relative alla trasparenza del trattamento dei dati personali suggeriscono come il legislatore europeo abbia inteso valorizzare tale aspetto secondo una prospettiva sensibilmente diversa rispetto alla precedente direttiva. Invero, la disciplina da quest'ultima predisposta si proponeva come strumento di restrizione della diffusione e della processazione dei dati personali rilasciati dal soggetto titolare[8]. In questa prospettiva, il profilo dell'accesso ai dati risultava pertanto intimamente connesso alle ragioni di controllo dell'informazione una volta fuoriuscita dalla sfera personale dell'individuo[9].

Nel rinnovato contesto tecnologico, la proliferazione di tecniche di processazione algoritmica di massa dei dati digitali ad alto contenuto personale e il successo di grandi imprese processanti basate sullo sfruttamento economico dei c.d. *big data*, hanno reso impellente l'attuazione di strumenti diversi da quelli finalizzati al controllo dei dati da parte del soggetto interessato. La enorme quantità dei dati disponibili e le notevoli capacità computazionali dei soggetti operanti nei mercati c.d. digitali[10] ha ben presto messo in luce l'insufficienza del consenso quale strumento di

---

[6] D. LIEBENAU, *What Intellectual Property can Learn from Informational Privacy, and Vice Versa*, in *Harvard Journal of Law & Technology*, 2016, 30, 1, 285 ss..

[7] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, OJ L 281, 23 Novembre 1995, 31–50.

[8] D. LIEBENAU, *What Intellectual Property can Learn from Informational Privacy, and Vice Versa,* cit., 297 ss..

[9] Cfr. R. GAVISON, *Privacy and the Limits of Law*, in *Yale. Law Journal*, 1980, 89, 421, 423, dove l'A. concettualizza la teoria della privacy come "accesso limitato" ai dati personali.

[10] Il potenziamento delle capacità computazionali delle imprese europee è stata notevolmente promossa anche dalla Commissione europea. Cfr. Staff Working Document, *Implementation of the Action Plan for the European High-Performance Computing Strategy*, SWD (2016) 106, 19 aprile 2016, reperibile online all'indirizzo https://ec.europa.eu/digital-single-market/en/news/staff-working-document-implementation-action-plan-european-high-performance-computing-strategy.

governo e di tracciabilità dei dati personali. A cascata, in un contesto di *massimizzazione* del trattamento dei dati risultano parimenti indeboliti i principi di necessità, di finalità e di proporzionalità che al contrario tendono a una *minimizzazione* dei dati trattati[11].

In diretta risposta ai mutamenti economici in corso, il Regolamento ha spostato il baricentro regolatorio, sotto il profilo soggettivo, dal soggetto interessato del trattamento ai soggetti titolari dello stesso trattamento[12], e sotto il profilo oggettivo, dal momento della collezione al momento successivo in cui le tecniche computazionali aggregano su larga scala e trattano i dati raccolti da varie fonti[13].

In questo quadro si collocano i nuovi obblighi che il Regolamento pone in capo alle imprese titolari del trattamento, con il fine di "procedimentalizzare" le attività imprenditoriali basate sulla processazione di dati personali[14]. Come sarà di seguito illustrato, si tratta di presidi informativi che mirano a rendere il trattamento 'verificabile' innanzitutto da parte del soggetto interessato, ponendo così le premesse per

---

[11] Cfr. art. 5.1 lett. c. RGDP.

[12] In questa prospettiva, taluna dottrina ha parlato di un'evoluzione della disciplina in materia di dati personali da un modello c.d. individual-based, ossia primariamente incentrato sul titolare dei dati, a un modello c.d. agent-based, diversamente incentrato sui soggetti che operativamente gestiscono il trattamento sui medesimi. B. VAN DER SLOOT, *The Individual In the Big Data Era: Moving towards an agent-based Privacy Paradigm,* in B. VAN DER SLOOT-D. BROEDERS-E. SCHRIJVERS, *Exploring the Boundaries of Big Data*, Amsterdam University Press, 2016, *passim*.

[13] Alla luce di questo cambio di prospettiva, si comprende come la disciplina della protezione dei dati abbia assunto, a seguito della riforma, la funzione di regola del comportamento di impresa, alla stregua del diritto antitrust. In questa prospettiva, sempre maggiori sono gli studi concernenti i contatti tra privacy e diritto antitrust, G. COLANGELO-M. MAGGIOLINO, *Data Protection in Attention Markets: Protecting Privacy Through Competition?*, in *Journal of European Competition Law & Practice*, 2017, 1 ss.; e che alcune autorità antitrust nazionali, in particolare quella tedesca, abbiano iniziato a indagare la connessione tra violazioni della disciplina in materia di dati personali e illeciti concorrenziali. Sul punto, G. SCHNEIDER, *Testing Art. 102 TFUE in the Digital Marketplace: insights from the Bundeskartellamt's Investigation against Facebook*, in *Journal of European Competition Law & Practice,* 9, 2018, 213 ss..

[14] A riguardo, si ricordano l'obbligo di tenuta dei registri del trattamento *ex* art. 30 RGDP, l'obbligo di notifica di una violazione dei dati personali all'autorità di controllo *ex* art. 33 RGDP, e la sua comunicazione all'interessato *ex* art. 34 RGDP, l'obbligo di valutazione dell'impatto del trattamento sulla protezione dei dati *ex* art. 35 RGDP e di consultazione preventiva dell'autorità di controllo in caso la valutazione d'impatto presenti un rischio elevato *ex* art. 36 RGDP.

l'azionabilità dei nuovi diritti positivi contenuti nello stesso Regolamento,[15] quali il diritto di opposizione[16], il diritto all'oblio[17], il diritto alla portabilità dei dati[18].
Nell'architettura del Regolamento, il principio di trasparenza è dunque venuto ad assumere un ruolo chiave in seno alla rinnovata disciplina in materia dei dati personali, permeando il ciclo di trattamento di dati dalla fase di progettazione delle tecnologie responsabili fino al momento del controllo successivo relativo alle conseguenze scaturenti dalle operazioni di processazione dei dati.

2.1 La prospettiva ex *ante: trasparenza e progettazione algoritmica*

Il principio di trasparenza opera innanzitutto in una prospettiva *ex ante* rispetto al trattamento, imponendo alle imprese processanti di progettare e strutturare le tecnologie algoritmiche in modo da renderle idonee a segnalare ai soggetti interessati le caratteristiche del trattamento. Le accortezze strutturali dovrebbero auspicabilmente investire le tre fasi principali del processo di trattamento dei dati: il momento della collezione e della archiviazione, della analisi e correlazione tra dati, e infine dell'output decisionale[19].
L'incorporazione delle ragioni di protezione dei dati fin dalla fase di costruzione delle tecnologie di trattamento è suggellata all'art. 25 RGDP, dove si richiede alle imprese di porre in essere "misure tecniche e organizzative adeguate" e di "integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare

[15] Così il considerando n. 39 RGDP: "è opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento".
[16] Art. 21 RGDP.
[17] Art. 17 RGDP.
[18] Art. 20 RGDP.
[19] *Ibid*.. Come osservato da alcuni autori, sotto il profilo economico, strutturare le tecnologie processanti ovvero servirsi di tecnologie connotate da certe caratteristiche demandate dal Regolamento dati personali, comporta notevoli costi per le imprese titolari del trattamento, con il connesso rischio di creare nuove barriere all'ingresso nei mercati digitali, che finirebbero per svantaggiare le piccole e medie imprese. B. GOODMAN, *A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union*, 2016, reperibile online all'indirizzo http://www.mlandthelaw.org/papers/goodman1.pdf, 6.

i diritti degli interessati"[20]. Proprio riguardo alla progettazione delle strutture processanti, l'art. 42 RDGP fa riferimento all'istituzione di "meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di *dimostrare* la conformità al presente regolamento dei trattamenti effettuati dai titolari e dai responsabili del trattamento"[21]. Come precisato a riguardo dal considerando n. 100 RGDP, tali meccanismi di certificazione delle tecnologie processanti dovrebbero consentire agli interessati "di *valutare rapidamente* il livello di protezione dei dati dei relativi a prodotti e servizi"[22].

Alla luce di queste disposizioni, il Regolamento sembra recepire il dibattito contemporaneo circa l'opportunità di architettare le tecnologie di processazione automatica dei dati secondo un *design* utente-centrico[23], in modo da incorporare per via strutturale ragioni di protezione della *privacy* che gli utenti sembrano ancora distanti dal tenere nella dovuta considerazione[24].

L'implementazione di un simile *design* potrebbe dunque incrementare la trasparenza delle operazioni di analisi dei dati non solo sotto un profilo quantitativo bensì qualitativo, ossia in termini di comprensibilità e intellegibilità delle informazioni sul trattamento rilasciate[25]. È quanto

---

[20] Ciò è stato interamente recepito dal considerando 78 RGDP, il quale fa espressa menzione di "misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni" del Regolamento, nonché, più precisamente, di "politiche interne e misure che soddisfino in particolare i principi della protezione dei dati *fin dalla progettazione e della protezione dei dati di* default". Corsivo aggiunto. Cfr. anche art. 24 RGDP relativo alla responsabilità dei titolari del trattamento.

[21] Corsivo aggiunto.

[22] Considerando n. 100 RGDP. Corsivo aggiunto.

[23] Cfr. S. DRISCOLL, *Applying Design Thinking to Law, Stanford Lawyer*, 94, 2016, reperibile online all'indirizzo https://law.stanford.edu/stanford-lawyer/articles/legal-design-lab-consumer-contracts/.

[24] V. studi comportamentali empirici su privacy, come quelli condotti da P. NORBERG-D. HORNE- D. HORNE, *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*, in *The Journal of Consumer Affairs*, 41, 1, 2007, 100-126. Sul punto si ricordino in particolare i rilievi di H. NISSEMBAUM, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Standford Law, 2010, 105, che lo afferma con riguardo a metodi di pagamenti scelti dai consumatori, comportamenti di acquisto, e scelte inerenti ai mezzi di comunicazione, osservando che le scelte in tali ambiti sono dettate più da ragioni di convenienza, di risparmio economico, e di connettività che da preoccupazioni di privacy. Come l'A. osserva, ciò può dipendere da vari fattori come la scarsa consapevolezza degli utenti stessi riguardo alle pratiche di collezione e processazione di dati condotte dalle società digitali, ed alle conseguenze da queste derivanti.

[25] Il considerando 39 RGDP richiede che siano accessibili alle persone fisiche "le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li

sottolineato anche dall'*Art. 29 Working Party*[26] nelle recenti linee guida ove la *Working Party* fa particolare leva sui c.d. strumenti di visualizzazione dell'informazione e di tecniche interattive per il rilascio delle medesime come mezzi per incrementare la trasparenza algoritmica[27]. Una posizione simile è stata adottata anche da alcune autorità garanti della *privacy* nazionali, quali quella inglese[28], le quali hanno parimenti messo in luce l'opportunità di rendere gli algoritmi processanti più trasparenti già a partire dalla loro costruzione.
Dal punto di vista tecnico, la sfida posta dal Regolamento è di portata notevole, posto che la strutturazione dei modelli matematico-informatici nel senso di una maggiore trasparenza va a scontrarsi direttamente con alcune proprietà strutturali degli attuali metodi di computazione di dati, complessi, sempre più autonomi dall'apporto umano e adattivi[29]. Queste proprietà rendono gli stessi metodi algoritmici in molti casi intrinsecamente oscuri alle facoltà cognitive umane[30].

2.2 La prospettiva ex *post: trasparenza e responsabilità*

Nella sistematica dei principi generali in materia dei dati personali, l'art. 5.1 RGDP affianca il principio di trasparenza al principio di liceità e

---

riguardano nonché la misura in cui i dati personali sono o saranno trattati". Ne deriva il diritto del soggetto titolare di ricevere "conferma e comunicazione" dei trattamenti dei dati personali che lo riguardano ed essere posto nelle condizioni di identificare l'identità del titolare del trattamento, nonché le finalità per le quali il medesimo trattamento viene svolto. Come precisato dal medesimo considerando, tali informazioni devono essere "facilmente accessibili" e "comprensibili", secondo un "linguaggio semplice e chiaro".

[26] L'Art. 29 Working Party era il comitato consultivo in materia di protezione dati personali interno alla Commissione ed era l'autorità centrale dei garanti della privacy nazionali. È interessante ricordare come dal 25 maggio 2018 l'Art. 29 *Working Party* sia stato sostituito dal Comitato europeo per la protezione dei dati ex artt. 68 ss. RGDP.

[27] WP 29, *Guidelines on Automated Individual Decision-Making and Profiling*, 22 Agosto 2018, 28, reperibile online all'indirizzo https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[28] UK International Commissioner's Office, *Discussion Paper on Profiling and Automated decision-making under the GDPR*, 13 aprile 2017, reperibile online all'indirizzo https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf.

[29] WP 29, *Guidelines on Automated Individual Decision-Making and Profiling*, cit., 8.

[30] Si ricordi in questo senso la celebre espressione "black box society" di F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, 2016, *passim*.

correttezza. Come alcuni considerando dichiarano[31], la trasparenza riguardante le operazioni di trattamento dei dati risponde a una *ratio* di governo dei rischi derivanti dalle pratiche di trattamento automatizzato. Assunto cardine della nuova disciplina è infatti che nell'economia degli algoritmi il trattamento automatizzato dei dati personali sia un'attività rischiosa[32], idonea a pregiudicare i diritti fondamentali dei soggetti titolari[33]. Questo perché il trattamento automatizzato dei dati personali fornisce il fondamento alle scelte decisionali di società operanti nei più diversi settori, da quello assicurativo, a quello creditizio[34]. La tutela dei dati personali, nella forma di una corretta collezione, corretta analisi e corretto impiego pratico dei medesimi, costituisce in questo senso precondizione della tutela dei diritti fondamentali dell'individuo coinvolti nei diversi processi decisionali[35]. È quello che il Regolamento chiaramente esplicita al considerando n. 78 RGDP, che fa riferimento ai rischi connessi al trattamento dei dati personali "per i diritti e le libertà delle persone fisiche", esposte a danni fisici, materiali o immateriali[36] potenzialmente derivanti dalle operazioni di trattamento[37].

---

[31] Cfr. considerando n. 39; 74; 75 RGDP.

[32] A. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in A. MANTELERO-D. POLETTI, *Regolare la tecnologia: il Reg. 2016/679 e la protezione dei dati personali. Un dialogo tra Italia e Spagna*, Pisa University Press, 2018, 289 ss.. ID., *Responsabilità e rischio nel Reg. UE 679/2016*, in *Nuove leggi civili commentate*, 1, 2017, 144 ss..

[33] Considerando n. 75 RGDP. Sulla connessione tra privacy e tutela dei diritti fondamentali G. COMANDE, *Tortious Privacy 3.0*: *a quest for research,* in J. POTGIETER-J. KNOBEL-R.M. JANSEN, *Essays in Honour of Huldigingsbundel vir Johann Neethling,* Durban, LexisNexis, 2015, 121 ss.. A. SPINA, *Risk Regulation of Big Data: Has the time arrived for a Paradigm shift in Eu Data Protection Law?, Case notes to Case C-293/12 and C-594/12* Digital Rights Ireland and Seitlinger and others, *cit.*, 248 ss..

[34] IS. RUBINSTEIN, *Big data: the end of privacy or a new beginning?,* in *International Data Privacy Law*, 2013, 3, 2, 74 ss., la quale parla di "rischi sistemici" ("systemic risks") derivanti dalle pratiche di processazione su larga scala di dati personali.

[35] G. COMANDE, *Tortious Privacy 3.0*: *a quest for research,* cit., 125.

[36] Così considerando n. 75 RGDP.

[37] Il considerando n. 78 RGDP identifica tra i possibili danni, "discriminazioni, furto o usurpazione di identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo". Il riconoscimento dell'intima connessione tra tutela dei dati personali e tutela di altri diritti ha lontane radici nelle prime concezioni di privacy americane, come *tort* creato proprio al fine di tutelare gli individui da pregiudizi causati dagli sviluppi tecnologici. S. WARREN-L. BRANDEIS, *The Right To Privacy*, in *Harvard Law Review*, 4, 5, 1980, 193 ss.; W. L. PROSSER, *Privacy*, in *California Law Review*, 1960, 48, 383 ss.. Sottolinea il punto anche D. J. SOLOVE, *A Taxonomy of Privacy*, in *University of Pennsylvania Law Review*, 2006,

Come i numerosi studi in materia di *data science* hanno messo in luce,[38] gli esiti dei processi di trattamento dei dati possono differire sensibilmente a seconda della composizione dei *dataset* iniziali che possono essere caratterizzati da c.d. *biases* perché incompleti, inesatti ovvero manipolati[39].
Ne deriva la necessità della creazione di strumenti giuridici volti a rendere le operazioni di trattamento dei dati verificabili sotto il profilo della liceità[40].
La verificabilità delle strutture algoritmiche processanti a sua volta risulta direttamente strumentale alla 'responsabilizzazione' delle imprese processanti (*accountability*), menzionata all'art. 5.2 RGDP, e relativa alla capacità delle stesse di dimostrare l'aderenza del trattamento svolto ai principi di correttezza e di liceità[41].
Così definito, il principio di responsabilizzazione delle imprese titolari del trattamento si articola lungo una duplice dimensione, interna ed esterna. Quella interna consiste nell'onere gravante sulle imprese digitali di adeguare i propri assetti tecnologici ai dettami della disciplina in materia di protezione dei dati, quali, ad esempio, i sopra citati obblighi di *privacy by design*. Quella esterna riguarda invece il passaggio successivo e consequenziale dell'abilità delle medesime di comunicare- e dunque di

---

154, 3, 477 ss.. Una simile concezione è stata più di recente espressa dalla *Commission Nationale de l'Informatique et des Libertés* che nel 2012 ha rilasciato un documento in cui si sottolinea esattamente la stretta connessione tra tutela della privacy e salvaguardia di altri beni giuridici, di carattere materiale, come di carattere immateriale. Più specificamente, la *Commission* nel documento fa menzione dei danni di carattere non solo pecuniario, ma anche morale, sociale e fisico potenzialmente causati dalla processazione dei dati. *Commission Nationale de l'Informatique e des libertés*, *Methodology for Privacy Risk Management*, June 2012 ed., reperibile online all'indirizzo https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf, 13.

[38] M. HARDT, *How Big Data is Unfair*, 26 Settembre 2014, reperibile online all'indirizzo https://medium.com/@mrtz/how-big-data-is-unfair-9aa544d739de.

[39] Per un'analisi dei riflessi giuridici, D. KAMARINOU-C. MILLARD-J. SINGH, *Machine Learning With Personal Data*, cit., 21; e già B. SCHERMER, *The Limits of Privacy in Automated Profiling and Data Mining*, in *Computer Law & Security Review*, 2011, 27, 11, 45 ss..

[40] Osservavano il punto già B. SCHERMER, *The Limits of Privacy in Automated Profiling and Data Mining*, cit., 45 ss. e M. HILDEBRANDT, *The Dawn of a Critical Transparency Right for the Profiling Era*, in J. BUS-M. CROMPTON-M. HILDEBRANDT- G. METAKIDES, *Digital Enlightment Book*, 2012, Amsterdam, IOS Press, 41 ss.. Cfr. il considerando n. 63 RGDP che precisa come il diritto di accesso consenta all'interessato di essere consapevole del trattamento e di verificarne la liceità.

[41] Di diverso avviso sembra al contrario A. MANTELERO, *Responsabilità e rischio nel Reg. UE 679/2016*, cit., 151, il quale distingue i tre diversi binari regolatori della trasparenza dei processi, la responsabilizzazione degli autori degli stessi e dell'adozione di forme di certificazione.

spiegare- ai soggetti interessati ovvero alle autorità di controllo, l'adesione alla disciplina *de quo*.
Come è evidente, tanto più alto è lo standard di trasparenza legislativamente sancito- e dunque più penetranti i riflettori esterni posti sulle attività di trattamento-, quanto maggiore è l'incentivo per le imprese processanti di osservare le norme poste a regolamentazione dei processi di trattamento. La trasparenza delle tecniche di trattamento algoritmico diviene in questa prospettiva veicolo di monitoraggio sulla *compliance* delle imprese digitali alla disciplina in materia dei dati personali[42]; e sul rispetto di quei principi di autonomia e non-discriminazione dell'individuo che la medesima disciplina si propone da ultimo di salvaguardare[43].

3. Le disposizioni sulla trasparenza nel Regolamento Generale Dati Personali

Le disposizioni relative alla trasparenza dei processi computazionali sono contenute nel capo III Sezione I del RGDP, intitolato "trasparenza e modalità". Conformemente, l'art. 12.1 RGDP demanda ai titolari del trattamento di implementare "misure appropriate" affinché le informazioni relative al trattamento siano rilasciate "in forma concisa, trasparente, intellegibile e facilmente accessibile".
Gli artt. 13 e 14 RGDP disciplinano gli obblighi di notifica gravanti sui titolari del trattamento, sulla base della distinzione tra dati raccolti dall'interessato e dati raccolti da altre fonti o altrimenti desunti attraverso il trattamento dei dati primari[44]. Al comma 1 le due disposizioni identificano le informazioni che i titolari del trattamento sono tenuti a rilasciare, riguardanti non solo l'identità del soggetto titolare del trattamento e del responsabile della protezione dei dati, le categorie dei dati processati, bensì anche le finalità e la base giuridica del trattamento. Similmente, l'art. 15 RGDP codifica il diritto di accesso dell'interessato a

[42] Non a caso il considerando n. 13 RGDP affianca obiettivi di "certezza del diritto e trasparenza degli operatori economici".
[43] Cfr. considerando n. 13 e 85 RGDP. Cfr. in via generale sul punto B. GOODMAN-S. FLAXMAN, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, 2016 ICML Workshop on Human Interpretability in Machine Learning, New York, WHI 2016, reperibile online all'indirizzo https://arxiv.org/abs/1606.08813, 3.
[44] Sulla distinzione tra dati primari e dati secondari si veda la classificazione di OECD, *Report on Data-Driven Innovation for Growth and Well-being,* 2015, reperibile online all'indirizzo https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf, 65.

un'ampia serie di informazioni, tra le quali informazioni relative ai soggetti a cui vengono disvelati i dati personali processati e al periodo di conservazione dei dati stessi[45].

Mediante il riferimento al diritto di accesso, il Regolamento si pone in linea di continuità con la precedente Direttiva che parimenti prevedeva il diritto in questione[46]. Il contenuto del diritto risulta tuttavia ampliato e reso più aderente al contesto tecnologico sottostante: l'art. 15, comma 1 lett. h RGDP sancisce infatti il diritto del soggetto interessato a conoscere l'"*esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par. 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*"[47]. Ai sensi degli artt. 13, 2 comma lett. f) e 14 RGDP, 2 comma lett. g), le medesime informazioni devono comunque essere rilasciate dal titolare del trattamento[48], a prescindere da un'apposita richiesta.

Nel contesto di operazioni di processazione basate su tecniche algoritmiche automatizzate, le disposizioni sull'accesso ai dati personali processati e alle informazioni relative al trattamento devono essere coordinate con le statuizioni di cui all'art. 22, 3 comma RGDP[49], ove è codificato il diritto dell'interessato non solo di "ottenere l'intervento umano da parte del titolare del trattamento, *ma anche quello di esprimere la propria opinione e di contestare la decisione*"[50]. La norma sottende l'obiettivo di creare una diretta

---

[45] Art. 15 RGDP. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, 7, 2, 76 ff. e J. POWLES- A. SELBST, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017, 7, 4, 233 ss.

[46] S. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation,* cit., 76 ss..

[47] Corsivo aggiunto.

[48] In via generale, la differenza tra il diritto di accesso *sub* art. 15 RGDP e i c.d. obblighi di notifica *sub* art. 13-14 RGDP sta nel fatto che mentre i secondi hanno ad oggetto informazioni che devono essere fornite all'interessato, il primo deve essere attivamente esercitato attraverso una richiesta specifica, che può essere inoltrata al titolare del trattamento anche dopo che la processazione automatizzata è stata condotta. La questione relativa a quando il diritto di accesso è azionabile è tuttavia dibattuta, cfr. S. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, cit., 76 ff. e J. POWLES- A. SELBST, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017, 7, 4, 233 ff..

[49] In questo senso, J. POWLES- A. SELBST, *Meaningful Information and the Right to Explanation*, in *International Data Privacy Law*, 2017, 7, 4, 233 ss. e G. MALGIERI-G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 4, 243 ss..

[50] Corsivo aggiunto.

interazione tra il titolare del trattamento e l'interessato del medesimo al fine di stimolare un intervento proattivo di quest'ultimo. In altri termini, la disposizione del 3 comma dell'art. 22 RGDP, contiene il diritto dell'interessato di verificare attivamente la processazione algoritmica dei suoi dati personali[51]. Tale diritto presuppone evidentemente che il soggetto interessato sia posto nelle condizioni di *conoscere* l'esistenza e i caratteri della processazione algoritmica che lo riguarda e di *comprendere* quindi le conseguenze da questa scaturenti[52].

Le informazioni relative alla logica utilizzata dallo strumento di processazione automatizzato, insieme all'importanza e alle conseguenze del trattamento previste, costituiscono l'oggetto di quello che la dottrina straniera ha denominato "diritto alla spiegazione algoritmica" ("right to explanation"). Questa espressione è desunta dal considerando n. 71 RGDP che espressamente afferma "il diritto (dell'interessato) (…) di ottenere una spiegazione della decisione (…) e di contestare la decisione"[53].

Il diritto alla spiegazione algoritmica è una delle più innovative risposte all'esigenza, percepita non solo in sede accademica[54] ma anche istituzionale[55] e professionale[56], di trovare nuovi strumenti di regolamentazione delle tecnologie di intelligenza artificiale.

---

[51] Sottolinea il punto C. KUNER ET AL., *Machine learning with personal data: is data protection law smart enough to meet the challenge?*, 2017, 7(1), in *International Data Privacy Law* , 1 ss., 2.

[52] In questo senso si esprimeva già M. HILDEBRANDT, *Who is Profiling Who? Invisible Visibility*, in S. GUTWIRTH-Y. POULLET-P. DE HERT- C. DE TERWANGNE- S. NOUWT, *Reinventing Data Protection?*, Dortdrecht-London, Springer, 2009, 239 ss., 248, ove l'A. osserva come i diritti aventi ad oggetto la contestazione di trattamenti automatizzati di dati si svuoterebbero (l'A. parla di "paper dragons") in assenza di adeguate informazioni relative a tale medesimo trattamento.

[53] B. GOODMAN-S. FLAXMAN, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, cit., 1 ss..

[54] M. HILDEBRANDT, *The New Imbroglio: Living with Machine Algorithms*, in L. JANSSENS, *The Art of Ethics in the Information Society,* Amsterdam University Press, 2016, 55 ss..

[55] Cfr. Le considerazioni mosse da EUROPEAN PARLIAMENT, *Briefing- Artificial Intelligence: Potential Benefits and Ethical Considerations*, Francesca Rossi Policy Department C: Citizens' Rights and Constitutional Affairs, Ottobre 2016, reperibile online all'indirizzo http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_BRI%282016%29571380; si vedano anche i rilievi mossi da INFORMATION COMMISSIONER'S OFFICE, *Overview of the General Data Protection Regulation (GDPR), Rights related to Automated Decision Making and Profiling*, House of Commons Publication, 2016, para. 46.

[56] Cfr. INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, *Is there a 'right to explanation' for Machine Learning in the GDPR?*, 1 Giugno 2017, reperibile online all'indirizzo https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/.

3.1 Il diritto alla "spiegazione algoritmica": il dibattito sulla natura sostanziale e funzionale

L'obbligo posto in capo a imprese processanti di rilasciare "informazioni significative sulla logica utilizzata" nel contesto di processi decisionali automatizzati ha destato l'attenzione della dottrina sin dalle prime bozze di proposte legislative[57].
Il dato normativo impone all'interprete il non agevole compito di mediare tra la vaghezza della nozione "informazione significativa sulla logica utilizzata" e le complessità strutturali delle tecnologie di *machine-learning*, connotate dalla dinamicità dei processi computazionali[58]. Simile complessità si traduce in un'imperscrutabilità costitutiva delle tecnologie in esame[59], che a sua volta determina l'incapacità degli utenti/consumatori di interpretare i processi di categorizzazione tracciati dagli algoritmi e gli effetti di tali medesimi processi[60].
La concreta azionabilità del diritto in questione- da taluni posta in dubbio[61]- deve essere valutata sul banco di prova della dimensione tecnologica, nel tentativo di identificare *quali* informazioni devono essere fornite al soggetto interessato per soddisfare il requisito della *significatività* delle informazioni relative alla logica dei processi automatizzati.
A riguardo, gli studiosi della materia si sono divisi tra coloro che si sono posti in maniera estremamente critica nei confronti del diritto in questione

---

[57] Sul punto vedi in particolare S. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, cit., 76 ff..

[58] La dinamicità delle nuove tecnologie di intelligenza artificiale risiede nella molteplicità delle fonti dei dati sulle quali l'algoritmo opera e sulla capacità di generare nuovi dati attraverso i processi automatizzati. C. KUNER ET AL., *Machine learning with personal data: is data protection law smart enough to meet the challenge?,* cit., 2.

[59] F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, cit., *passim*; ID., *Secret Algorithms Threaten Rule of Law*, in *Mit Technology Review*, 2017, 1, reperibile online all'indirizzo https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/. È quanto da ultimo sottolineato anche da WP 29, *Guidelines on Automated Individual Decision-Making and Profiling,* cit., 17.

[60] S. GUTWIRTH- M. HILDEBRANDT, *Some Caveats on Profiling*, in S. GUTWIRTH- P. DE HERT- Y. POULLET, *Data Protection in a Profiled Age*, New York, Springer, 2010, 36.

[61] *Ex multis*, J. BURRELL, *How the machine "thinks": Understanding opacity in machine learning algorithms*, in *Big Data Society*, 2016, 3(1), reperibile online all'indirizzo http://bds.sagepub.com/content/3/1/ 2053951715622512.

e altri che lo hanno positivamente accolto quale interessante strumento di responsabilizzazione delle imprese operanti nel digitale. Più precisamente, il diritto alla spiegazione algoritmica di cui agli artt. 13-15 RGDP è stato variamente interpretato i) come diritto di accedere all'algoritmo responsabile di un certo trattamento;[62] ii) come diritto a ottenere informazioni riguardanti le funzionalità sistemiche delle strutture algoritmiche processanti[63]; ovvero iii) come diritto dell'interessato a ottenere informazioni inerenti una singola specifica decisione effettuata dall'impresa sulla base dei propri sistemi di processazione automatizzata[64].
Secondo una prima posizione,[65] le previsioni riguardanti la trasparenza algoritmica contenute nel Regolamento sottenderebbero una "fallacia" di fondo simile a quella che è venuta a connotare lo strumento del consenso nella dimensione digitale: si tratterebbe, cioè, di diritti "immaginari" che non assicurano al soggetto interessato un reale controllo circa il trattamento che lo riguarda. In questa prospettiva, il diritto alla spiegazione algoritmica, come codificato nel Regolamento, postulando il rilascio di informazioni tecniche che il soggetto interessato medio comunque non potrebbe essere in grado di comprendere, non consentirebbe a questi di conseguire un controllo effettivo sul trattamento automatizzato che lo riguarda[66]. In base a tale interpretazione, quindi, l'introduzione di diritti all'informazione nel contesto algoritmico altro non sarebbe che un'operazione normativa di facciata, idonea a coprire solamente in superficie gli squilibri di potere sussistenti tra utenti e imprese processanti[67].
Seguendo la medesima linea critica, un altro filone dottrinale[68] ha inteso circoscrivere le informazioni oggetto dell'obbligo di rilascio unicamente alle

---

[62] L. EDWARDS- M. VEALE, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably not the Remedy you are Looking for*, in *Duke Law and Technology Review*, 2017, 16, 1, 18 ss.; B. GOODMAN-S. FLAXMAN, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"*, cit., 6.
[63] WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation,* cit., 77 ss..
[64] J. POWLES- A. SELBST, *Meaningful Information and the Right to Explanation*, cit., 233 ss..
[65] L. EDWARDS- M. VEALE, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably not the Remedy you are Looking for*, cit., 65 ss..
[66] D. KAMARINOU-C. MILLARD-J. SINGH, *Machine Learning With Personal Data*, cit., 13, ove viene fatto riferimento al codice sorgente.
[67] L. EDWARDS- M. VEALE, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably not the Remedy you are Looking for*, cit., 67.
[68]WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation,* cit., 77 ss..

informazioni relative alle *funzionalità sistemiche* della struttura algoritmica processante[69]. Le informazioni che il Regolamento richiede trasparenti riguarderebbero unicamente le funzionalità generali dei trattamenti automatizzati, ossia le specifiche relative ai requisiti funzionali, ai modelli predefiniti utilizzati, ai criteri e alle strutture di classificazione, e infine ai c.d. alberi decisionali[70].

Un ultimo indirizzo dottrinale[71] ha infine proposto di interpretare la clausola generale di significatività delle informazioni che il titolare del trattamento deve rilasciare, a partire dal punto di vista del soggetto interessato. Secondo questa prospettiva, dovrebbero considerarsi significative unicamente quelle informazioni che un soggetto medio non dotato di conoscenze tecniche sarebbe in grado di comprendere.

Più precisamente, la dottrina in esame intende proporre un'interpretazione *strumentale* della nozione di significatività delle informazioni, considerando "significative" unicamente quelle informazioni che pongono l'interessato nella condizione di attivarsi per esercitare correttamente gli altri diritti positivi previsti dalla disciplina in materia dei dati personali, e in particolare, quello di contestare la decisione effettuata sulla base del trattamento automatizzato. Le informazioni sulla logica del trattamento automatizzato costituenti l'oggetto del diritto alla spiegazione *ex* artt. 13-15 RGDP, sarebbero pertanto "significative" unicamente se *funzionali* ad un esercizio attivo della facoltà di autodeterminazione del soggetto interessato attraverso l'esercizio dei diritti previsti dal Regolamento.

Il rilascio di informazioni riguardanti la processazione algoritmica rientrerebbe in questo senso nell'obbligo posto in capo ai titolari del trattamento di "agevolare" l'esercizio dei diritti dell'interessato[72].

L'interpretazione in senso strumentale della nozione di significatività delle informazioni riguardanti i trattamenti algoritmici, risulta alquanto utile al

---

[69] *Ibid*., 79-84. Tale interpretazione è basata sul fatto che gli artt. 13; 14 e 15 RGDP fanno riferimento al rilascio di informazioni relative, tra le altre, alle "conseguenze *previste* del trattamento": secondo tale lettura pertanto, il riferimento alle "conseguenze *previste*" sottenderebbe implicitamente la volontà da parte del legislatore di restringere il novero delle informazioni oggetto dell'obbligo di notifica e del diritto di accesso.

[70] Simile lettura è stata di rimando notevolmente criticata sulla base dell'osservazione che i caratteri sistemici dell'algoritmo definiscono anche le specifiche decisioni incidenti sulla sfera individuale degli utenti/consumatori. Cfr.J. POWLES- A. SELBST, *Meaningful Information and the Right to Explanation*, cit., 233 ss..

[71] *Ibid*., 236.

[72] Così art. 12 RGDP.

fine di individuare le informazioni oggetto dell'obbligo di rilascio. Essa suggerisce l'opportunità di una determinazione caso per caso delle informazioni "sulla logica del trattamento automatizzato", avuto riguardo da un lato alle specifiche proprietà dei sistemi di *machine learning* responsabili del trattamento automatizzato e dall'altro alle caratteristiche individuali del soggetto interessato. In questo senso sarebbe ad esempio auspicabile la definizione delle informazioni da considerarsi "significative" ai sensi delle norme in commento per mezzo di codici di condotta[73] opportunamente declinati a seconda delle "specificità" dei settori economici di riferimento.

3.2 Le informazioni sulla logica utilizzata dal trattamento automatizzato: dalla spiegazione alla verificabilità algoritmica

Una proposta di definizione delle informazioni che le imprese titolari del trattamento sono tenute a rilasciare ai sensi degli artt. 13-15 RGDP è stata fornita dall'*Art. 29 Working Party* nelle c.d. *Good Practice Recommendations*[74]. Secondo la *Working Party* sono da considerarsi informazioni "significative sulla logica utilizzata" le informazioni relative ai dati impiegati per la profilazione, alle fonti originarie di questi dati, alle modalità di strutturazione del profilo impiegato nel processo decisionale, alla rilevanza di tale medesimo profilo ai fini decisionali[75]. In base a questa interpretazione, sarebbero inoltre oggetto dell'obbligo di *disclosure* i criteri decisionali utilizzati dall'impresa[76], ossia i criteri di correlazione e categorizzazione, in base ai quali, a loro volta, viene valutato il profilo del soggetto interessato dal processo decisionale[77].

---

[73] I codici di condotta sono espressamente presi in considerazione all'art. 40, 1 comma RGDP: "Gli Stati Membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione della specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese".

[74] WP 29, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, adottate il 3 Ottobre 2017, 28 ss..

[75] *Ibid.*, 28.

[76] Art. 29 Data Protection Working Party, *Opinion 3/2013 on Purpose Limitation*, 2 Aprile 2013, reperibile online all'indirizzo https://ec.europa.eu/newsroom/article29/news-overview.cfm, 47.

[77] Art. 29 Data Protection Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679,* cit., 28. Cfr. Anche J. BURRELL, *How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms*, cit., 1-2.

Secondo la lettura data, sarebbero pertanto idonee a soddisfare il requisito della significatività di cui agli artt. 13-15 RGDP, quelle informazioni che una parte di dottrina ha definito informazioni relative alla implementazione degli algoritmi[78], ossia relative alla operatività dei medesimi nel contesto commerciale di riferimento. Rientrano in questa categoria le informazioni relative alle finalità per cui vengono raccolti i dati processati, alla natura commerciale o non commerciale della stessa, ai dati personali rilevanti ai fini della decisione ultima presa[79].

A riguardo, sono indicative le precisazioni del considerando n. 63 dello stesso Regolamento, che in relazione al diritto di accesso del soggetto interessato, afferma come questi abbia diritto a conoscere e "ottenere comunicazioni relative in particolare alle finalità in relazione a cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato di dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento".

Alla luce delle considerazioni sopra svolte, il requisito della significatività delle informazioni sembra dover essere positivamente avvalorato al fine di circoscrivere il carico informativo gravante sulle imprese processanti sì da evitare un *information overload* disfunzionale[80].

A riguardo, taluna dottrina ha suggestivamente proposto di interpretare la nozione di significatività sul trattamento algoritmico alla stregua di intellegibilità, per cui dovrebbero essere rilasciate ai sensi del Regolamento unicamente quelle informazioni relative ai metodi computazionali di trattamento che un soggetto interessato medio potrebbe comprendere autonomamente[81]. Simile interpretazione è del resto suggerita dallo stesso art. 12 RGDP che richiede al soggetto titolare del trattamento di fornire le

---

[78]La distinzione tra informazioni relative all'architettura degli algoritmi processanti e alla implementazione degli stessi è formulata da G. COMANDÈ-G. MALGIERI, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* in *International Data Privacy Law*, 2017, 7, 4, 243 ss..

[79] *Ibid*., 245.

[80]Un'interpretazione eccessivamente estensiva delle norme sulla trasparenza algoritmica rischierebbe di far emergere le medesime problematiche tradizionalmente relative alle informative sulla privacy, e più specificamente relative alla lunghezza e alla complessità tecnica delle medesime.

[81]G. COMANDÈ-G. MALGIERI, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* cit., 245.

informazioni relative al trattamento in maniera "concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro". Sembrano pertanto doversi escludere dal raggio applicativo delle disposizioni sulla trasparenza algoritmica le informazioni tecniche relative alle funzionalità sistemiche dell'algoritmo: le informazioni di natura più tecnica relative alle caratteristiche della architettura processante, come il codice sorgente, non sarebbero infatti idonee a soddisfare il requisito di significatività di cui agli artt. 13-15 RGDP, in quanto non fruibili dall'utente.

Queste ultime informazioni potrebbero al contrario essere rilevanti ai fini del c.d. *auditing* algoritmico condotto da terzi esperti[82]. Le operazioni di *audit* sono funzionali al monitoraggio e alla verificabilità della struttura algoritmica, con il fine precipuo di individuare i *bias* inficianti il ciclo algoritmico[83]. Si tratta dunque di vere e proprie investigazioni tecniche relative ai meccanismi di funzionamento interno delle architetture computazionali processanti massicce moli di dati[84].
Il potere di "condurre indagini sotto forma di attività di revisione sulla protezione dei dati" è assegnato *ex* art. 58, 1 comma lett. a) RGDP alle autorità di controllo nazionali. Dalla stessa disposizione si desume come ai fini della revisione algoritmica, le stesse autorità hanno anche il potere di "ottenere dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie" per

---

[82]B. GOODMAN, *A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union*, cit., 4 ss. Cfr. anche B. MITTELSTADT, *Auditing for Transparency in Content Personalization Systems*, in *International Journal of Communication*, 2016, 10, 4991 ss., ove l'A. definisce l'auditing algoritmico come il processo di indagine delle proprietà funzionali e degli effetti delle decisioni prese in conformità ai trattamenti algoritmici. Attraverso l'*auditing* è dunque possibile prevedere i risultati derivanti da nuovi *input* e ottenere pertanto una spiegazione della logica sottostante le medesime decisioni, relativa ad esempio al perché un dato input ha determinato una data classificazione.
[83]B. CASEY-A. FARHANGI- R. VOGL, *Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise*, in *Berkeley Technology Law Journal* (in prossima uscita), reperibile online all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325, *passim*.
[84] ART.29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679,* cit., 32, dove l'auditing è definito funzionale al "testing the algorithms used and developed by machine learning systems to prove that they are actually performing as intended and not producing discriminatory, erroneous or unjustified results". Per la dottrina si rimandi a P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Decision Making in the EU Law*, in *Common Market Law Review*, 2018, 55, 1143 ss., 1170-1173.

l'esecuzione di tale compito investigativo[85]. A tale potere di indagine delle autorità di controllo corrisponde il dovere delle società processanti di condurre le c.d. "valutazioni d'impatto sulla protezione dei dati e consultazione preventiva" di cui all'art. 35 RGDP. Si tratta di un documento di mappatura dei rischi "per i diritti e le libertà delle persone fisiche" insiti in un trattamento che prevede "l'uso di nuove tecnologie". Tale documento dovrà essere redatto prima che il trattamento medesimo sia condotto e contenere, oltre a "una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento (…)"[86] e a una "valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità"[87], la descrizione delle "*misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento* (…)"[88]. La disposizione in commento richiede pertanto una descrizione dettagliata delle informazioni strutturali e dunque architetturali degli algoritmi processanti[89].

Come osservato dall'*Art. 29 Working Party*, ai fini di un esito positivo della valutazione d'impatto è importante che le imprese implementino procedure e misure funzionali alla *prevenzione* di errori, imprecisioni e fattori discriminanti nel corso del trattamento[90]. In questa prospettiva, meglio si comprende la rilevanza dell'incorporazione di principi di protezione di dati personali nel *design* delle strutture algoritmiche processanti[91].

L'obbligo di valutare l'impatto di un trattamento condotto per mezzo di "nuove tecnologie"[92] richiede dunque alle imprese operanti con i dati digitali di tenere sotto controllo le proprietà tecniche dei metodi computazionali impiegati, al fine ultimo di individuare le eventuali fonti dei danni per i soggetti interessati dal trattamento.

---

[85] Art. 58,1 comma lett. e) RGDP.
[86] Art. 35, 7 comma lett. a) RGDP.
[87] Art. 35, 7 comma lett. b) RGDP.
[88] Art. 35, 7 comma lett. d) RGDP. Corsivo aggiunto.
[89] Cfr. ARTICLE 29 DATA PROTECTION WORKING PARTY 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/769*, adottato il 4 Aprile 2017, 17-18.
[90] WP 29, *Guidelines on Automated Individual Decision-Making and Profiling*, cit., 28.
[91] Cfr. quanto osservato *supra* para 2.1. Tra i principi in materia di "data protection by design" si ricordano, ad esempio, il principio di pseudonimizzazione e il principio della minimizzazione dei dati.
[92] Cfr. art. 35 RGDP.

Le valutazioni d'impatto possono essere condotte nella forma di *audit* interni o esterni[93], ossia da parte di soggetti interni ovvero esterni all'impresa titolare. In quest'ultima ipotesi, le imprese terze dovranno essere poste nelle condizioni di verificare adeguatamente la regolarità delle operazioni di trattamento mediante il trasferimento di informazioni commercialmente sensibili relative alle strutture algoritmiche.
A riguardo è stato osservato come la variante dell'*auditing* esterno potrebbe favorire pratiche collusive tra le imprese che effettuano l'*auditing* e quelle che lo subiscono, con il connesso rischio che si formino dei quasi-monopoli di poche grandi società deputate alla verificazione algoritmica[94].
Quello della valutazione d'impatto è uno strumento estremamente importante per il perseguimento di una maggiore trasparenza relativa ai trattamenti algoritmici, in primo luogo perché impone alle imprese titolari della processazione di esaminare e descrivere le operazioni di trattamento svolte. Il documento risultante è inoltre oggetto di diretta verifica da parte delle autorità di controllo[95]. Ai sensi dell'art. 36, 1 comma RGDP, infatti, l'impresa titolare del trattamento deve consultare l'autorità di controllo "qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio", e in tale caso è tenuta a comunicare all'autorità di controllo "la valutazione d'impatto e tutte le informazioni necessarie". La norma in commento sembra pertanto porre in capo al titolare del trattamento un vero e proprio dovere di collaborazione nei confronti dell'autorità di controllo, che deve essere a maggior ragione osservato nel corso delle indagini condotte dalla medesima autorità *ex* art. 58 RGDP.

---

[93] ART. 29 DATA PROTECTION WORKING PARTY, *Working Document Setting up a table with the elements and principles to be found in binding corporate rules*, adottato il 29 novembre 2017, reperibile online all'indirizzo https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109, 12.

[94] Così GOODMAN, *A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union*, cit., 6, il quale opera un paragone con il monitoraggio nei mercati finanziari. È stata anche avanzata in dottrina l'ipotesi della creazione di una autorità indipendente appositamente deposta al monitoraggio algoritmico. Cfr. L. EDWARDS- M. VEALE, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably not the Remedy you are Looking for*, cit., 83-84. In prospettiva europea, si rimandi a S. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation,* cit., 98.

[95] 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,* cit., 36-37.

In questa prospettiva, dal combinato disposto degli artt. 35; 36 e 58 RGDP sembra potersi desumere l'obbligo di rendere il trattamento automatizzato verificabile da parte dell'autorità di controllo. Si tratta di un diritto di accesso alla struttura algoritmica processante diverso dal diritto di spiegazione *ex* artt. 13-15 RGDP, avente ad oggetto informazioni più sofisticate dal punto di vista tecnico.
Dal quadro normativo sin qui tratteggiato emerge come le disposizioni in materia di trasparenza algoritmica possano essere suddivise in due categorie: le prime relative al diritto di spiegazione *ex* artt. 13-15 RGDP, avente come destinatario il singolo soggetto interessato del trattamento e come oggetto le informazioni relative alla rilevanza pratica del trattamento automatizzato, di natura intellegibile per il soggetto interessato; le seconde relative alla verificabilità delle caratteristiche strutturali della architettura computazionale da parte di soggetti terzi esperti, l'autorità di controllo *ex* art. 58 RGDP ovvero società terze *ex* art. 35 RGDP.

4 . L'altra faccia dell'algoritmo: la tutela del segreto commerciale

Ai fini della delimitazione dell'ambito applicativo delle previsioni in materia di trasparenza algoritmica contenute nel Regolamento dati personali, rilevante appare il considerando n. 63 RGD: è qui precisato che "ove possibile il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto 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".
Il Regolamento dati personali, seppure unicamente a livello di considerando, sembra così introdurre un'eccezione alle disposizioni in materia di trasparenza algoritmica sopra commentate[96].

[96] È stato a riguardo osservato come il considerando 63, riferendosi unicamente al diritto di accesso del soggetto interessato, riguarderebbe unicamente la previsione di cui all'art.15 RGDP e non invece altre disposizioni in materia di trasparenza, come gli obblighi di notifica ex artt. 13-14 RGDP o ancora le sopra esaminate disposizioni di cui agli artt. 35; 36 e 58 RGDP. In relazione a tali disposizioni il Regolamento sembrerebbe non prendere in considerazione la possibilità di un contrasto con i diritti di proprietà intellettuale. Così G. MALGIERI-G. COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation,* cit., 263, secondo cui gli obblighi di notifica *ex* artt. 13-14 RGDP non dovrebbero dunque essere limitati in alcun caso. Ad avviso di chi scrive,

Invero, le informazioni tecniche relative alla "logica utilizzata" dal trattamento automatizzato costituiscono indubbiamente un *asset* immateriale estremamente prezioso per le imprese che operano nei mercati digitali. In quanto tali, le stesse informazioni oggetto delle disposizioni di cui al Regolamento dati personali ricadono sotto la tutela dei diritti di proprietà industriale e, segnatamente, del segreto commerciale e del diritto autoriale sul software.

Si profila pertanto un delicato problema di bilanciamento tra due diverse categorie di diritti, da un lato quelli individuali di accesso alle informazioni trattamento automatizzato, e dall'altro i diritti industriali aventi ad oggetto le informazioni relative alla processazione automatizzata di dati personali. A riguardo, è interessante osservare come il considerando n. 4 RGDP abbia cura di precisare che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità". Tra i diritti fondamentali menzionati dal medesimo considerando si rinviene proprio quello della libertà di impresa[97].

Il contemperamento suggerito dal citato considerando richiede dunque innanzitutto un esame circa i diritti di proprietà intellettuale insistenti sulle informazioni relative alla logica utilizzata dal trattamento automatizzato. Invero, sebbene vi siano alcuni sistemi algoritmici *open source*[98], la maggior parte delle strutture processanti automatizzate e delle informazioni da queste processate sono tutelate dal segreto commerciale[99].

In un contesto economico sempre più basato sulla conoscenza anziché sul prodotto[100] e che pone gli *asset* immateriali al centro delle dinamiche concorrenziali[101], le imprese operanti nel mercato digitale ricorrono in via

---

un'interpretazione teleologica del considerando, come più generalmente comprensiva delle previsioni di trasparenza appare più appropriata.

[97] Sulla tutela della libertà d'impresa nella economia digitale, si rimandi alle statuizioni della COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni 'Verso una florida economia europea basata sui dati"*, 2 luglio 2014, COM(2014), 442, 2.

[98] Il modello algoritmico *open source* è usato specialmente nel settore biomedico.

[99] Cfr. N. SHEMTOV, *Beyond the Code: Protection of Non-Textual Features of Software*, Oxford University Press, Oxford, 2017, 220.

[100] D. FORAY, *Economics of Knowledge*, Cambridge, 2004, 141 ss..

[101] J. REICHMAN, *Of Green Tulips and Legal Kudzu: Repackaging Rights in Subpatentable Innovation,* 53, 6 Vanderbilt Law Review, 2000, 1743 ss.. Cfr. C. SHAPIRO-H. R. VARIAN, *Information rules- Le regole dell'economia dell'informazione*, Milano, 1999, *passim.*

sempre maggiore a schemi di tutela basati sulla segretezza del *know-how* piuttosto che sulla protezione brevettuale[102].

La segretezza del *know-how* viene infatti considerata, in molti casi, economicamente più vantaggiosa e dunque preferibile alla privativa brevettuale[103]: ciò è dovuto in prima istanza ad alcune differenze *strutturali* intercorrenti tra la protezione brevettuale e quella del *know-how*, direttamente relative alla natura non titolata del diritto avente ad oggetto il *know-how*[104]. Questo, non soggetto a gravosi oneri di registrazione, sorge automaticamente in presenza dei requisiti fissati dalla legge[105].

In relazione allo specifico caso delle strutture algoritmiche processanti è necessario inoltre ricordare come l'ufficio europeo dei brevetti abbia qualificato le stesse come metodi matematici, escludendone dunque la natura di invenzioni rilevanti a fini brevettuali[106]. Ne è derivata la necessità per le imprese titolari del trattamento di affidarsi ad altri strumenti di tutela.

---

[102] GOY-WANG, *Does knowledge tradeability make secrecy more attractive than patents? An analysis of IPR strategies and licensing, Oxford Economic Papers,* 68, 2016, 64 ss.; cfr. anche J. POOLEY, *Trade Secrets: the other IP right*, in *Wipo Magazine*, 2013, 3 e A.A. SCHWARTZ, *The Corporate Preference for Trade Secret*, in *Ohio State Law Journal*, 2013, 74, 624 ss..

[103] In questo senso si è espressa la Commissione Europea, nello *Study on Trade Secrets and Confidential Business Information in the Internal Market,* pubblicato ad Aprile 2013, reperibile online all'indirizzo http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf (ultimo accesso 1 maggio 2017), 87-88.

[104] A. VANZETTI- V. DI CATALDO, *Manuale di diritto industriale,* Milano, 2009, 489-490.

[105] Sul punto M. A. LEMLEY, *The surprising virtues of trade secret sas IP rights,* Stanford Law and Economics Olin Working Papers n. 358, 2008, reperibile online all'indirizzo https://web.stanford.edu/dept/law/ipsc/pdf/lemley-mark.pdf, *passim*. Definiscono il segreto come "mero fatto", A. VANZETTI- V. DI CATALDO, *Manuale di diritto industriale,* cit., 489. Sui rapporti tra brevetto e segreto, si rimandi alle osservazioni di K. CZAPRACKA, *Antitrust and Trade Secrets: the U.S. and the EU Approach*, in *Santa Clara Computer and High Technology Law Journal*, 2007, 216-218, dove si riconosce la funzione di 'gap-filling' del segreto rispetto al brevetto.Cfr. anche B.M. SIMONS- T. SICHELMAN, *Data-generating Patents*, in *Northwestern University Law Review*, 2016, 111, 2, 377 ss..

[106] Cfr. Camera di appello dell'ufficio europeo dei brevetti, T-1748/06, 28 gennaio 2009, *Classification Method/Compel*, reperibile online all'indirizzo https://www.epo.org/law-practice/case-law-appeals/pdf/t061748eu1.pdf. Per la dottrina G. NOTO LA DIEGA, *Against the Dehumanisation of Decision-Making- Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, 9, 3 ss., 15. Come osservato in dottrina, un algoritmo non potrebbe essere oggetto di tutela brevettuale posto che questa non può insistere su idee o su modelli di business, che devono rimanere nel pubblico dominio. Così J. DREXL-R.M. HILTY-L. DESAUNETTES-F. GREINER- D. KIM- H. RICHTER- G. SURBLYTÉ-K. WIEDEMANN, *Data ownership and Access to Data, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*, reperibile online all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165, 5-6.

La crescente importanza economica degli *asset* informativi ha avuto riflessi diretti sul piano giuridico, con l'ingresso e la presa di campo di strumenti di tutela che si distinguono dal brevetto sotto il triplice profilo dell'*oggetto* (*i.e.* non già invenzioni, bensì informazioni "pure"), della *struttura* della protezione (*i.e.* segretezza, anziché privativa di mercato) e, da ultimo, della *funzione* della stessa tutela (*i.e.* riservatezza del dato informativo anziché trasparenza del medesimo)[107].

Il conferimento di una tutela specifica al dato informativo è funzionale ad incentivare le imprese ad investire in attività di ricerca e sviluppo consistenti nella raccolta e nella elaborazione di informazioni che seppur non brevettate contribuiscono al progresso innovativo[108].

In questo quadro si colloca la riforma europea in materia di segreti commerciali, consumatasi con l'emanazione della Direttiva UE 943/2016[109], volta ad armonizzare la tutela delle informazioni commerciali riservate sul territorio europeo[110].

La riforma è venuta ad accordare al *know-how* una tutela ben maggiore di quella relativa alla concorrenza sleale demandata dallo standard

---

[107] Sul punto M. LIBERTINI, *Tutela e promozione delle creazioni intellettuali e limiti funzionali della proprietà intellettuale*, in *AIDA*, 1, 2014, 299 ss., 316 e A. VANZETTI, *La tutela "corretta" delle informazioni segrete,* in Riv. Dir. Ind., I, 2011, 95 ss.. Cfr. anche R. MORO VISCONTI, *La valutazione economica del know-how,* in *Il diritto industriale,* 2012, 369 ss., 372 e similmente anche R. ROMANO, *L'innovazione tecnica tra diritti titolati e diritti non titolati (dalla creazione alla segretazione)?,* in S. GIUDICI (a cura di), *Studi in Memoria di Paola A. E. Frassi*, Giuffrè, Milano, 2010, 607 ss..

[108] M. LIBERTINI, *Le informazioni aziendali segrete come oggetto di diritti di proprietà intellettuale, in Riv. It. Scienze giuridiche*, 2011, 137 ss.. Sul punto anche S. MAGELLI, *Il know-how nell'esperienza giurisprudenziale italiana tra esclusiva e concorrenza sleale*, in *Il diritto industriale*, 2, 2016, 189 ss..

[109] Per un commento generale, si veda D. ARCIDIACONO, *Prospettive di adeguamento del diritto italiano alla direttiva Trade Secrets,* in Orizzonti del diritto commerciale, 2016, 2, reperibile online all'indirizzo http://www.rivistaodc.eu/edizioni/2016/2/saggi/prospettive-di-adeguamento-del-diritto-italiano-alla-direttiva-trade-secrets/.

[110] Sul punto, MAX PLANCK INSTITUTE FOR INNOVATION AND COMPETITION, *Comments of 3 June 2014 on the Proposal of the European Commission for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure of 28 November 2013, COM(2013) 813 final*, reperibile online all'indirizzo https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/translation_stellungnahme_tsp_mpi_clear_af_with_changes_01.pdf, 1-2. Cfr. anche i rilievi di V. FALCE, *Tecniche di protezione delle informazioni riservate. Dagli accordi TRIPs alla direttiva sul segreto industriale*, in *Riv. dir. ind.*, 2016, 129 ss..

internazionale di cui all'art. 39.2 TRIPS[111] e definibile come quasi-privativa[112].

La Direttiva definisce segreto commerciale informazioni "i) che sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; ii) hanno valore commerciale in quanto segrete; iii) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, atte a mantenerle segrete"[113].

La tutela del segreto commerciale riguarda l'"acquisizione, l'utilizzo, o la divulgazione illeciti del loro segreto commerciale" e garantisce il "risarcimento per tale acquisizione, utilizzo o divulgazione"[114]. L'illiceità della acquisizione, utilizzo o divulgazione dell'informazione deriva dalla *mancanza di consenso del detentore del segreto commerciale* e dal fatto che l'autore abbia acquisito il segreto commerciale "in via illecita; abbia violato un accordo di riservatezza o qualsiasi altro obbligo di non divulgare il segreto commerciale; ovvero abbia violato un accordo contrattuale o di altra natura che impone limiti all'utilizzo del segreto commerciale"[115]. Il riferimento al consenso del detentore del segreto commerciale echeggia logiche proprietarie[116], a cui il legislatore della riforma, malgrado le

---

[111] L'art. 39, 2 dell'Accordo TRIPS, richiede agli Stati Membri di garantire una protezione minima al *know-how* limitatamente ad attività risultanti contrarie "alle leali pratiche commerciali": "*le persone fisiche e giuridiche hanno la facoltà di vietare che, salvo proprio consenso, le informazioni sottoposte al loro legittimo controllo siano rivelate a terzi oppure acquisite o utilizzate da parte di terzi in un modo contrario a leali pratiche commerciali nella misura in cui tali informazioni: a) siano segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; b) abbiano valore commerciale in quanto segrete; e c) siano state sottoposte, da parte della persona al cui legittimo controllo sono soggette, a misure adeguate nel caso in questione intesa a mantenerle segrete*". La definizione dell'espressione "*leali pratiche commerciali*" deve desumersi dall'art. 10 bis della Convenzione di Parigi per la protezione della proprietà industriale. Sul punto V. FALCE, *Trade Secret Protection in the Innovation Union*. *From the Italian Approach to the UE Solution,* in *Diritto, Mercato e Tecnologia*, 4, 2013, 20 ss..

[112] Cfr. A. OTTOLIA, *Big Data e innovazione computazionale*, Quaderni di Aida n. 28, Torino, Giappichelli, 2017, 49-50.

[113] Art. 2, 1 comma Direttiva UE 943/2016.

[114] Art. 4 Direttiva UE 943/2016.

[115] Art. 4, 2 comma Direttiva UE 943/2016.

[116] Per un commento sia consentito il rimando a T. APLIN, *Confidential Information as Property?*, in *King's Law Journal*, 2013, 2, 172 ss. e ID., *Right to Property and Trade Secrets*, in

dichiarazioni di cui ai considerando[117], sembra ispirarsi, sulla falsariga di quanto era già avvenuto in alcuni ordinamenti nazionali, come quello italiano[118].
Dalle disposizioni citate emerge come la nuova direttiva abbia imposto agli stati membri uno standard di tutela particolarmente alto, a partire dalla nozione di segreto commerciale suscettibile di comprendere un'innumerevole quantità di informazioni commerciali, ad esclusione solamente, come precisato dal considerando n. 14, delle "informazioni trascurabili" e dunque di scarsa importanza economica.
La disciplina così configurata consente pertanto alle imprese che operano mediante l'utilizzo di strumenti di trattamento automatizzato di dati personali di proteggere una buona parte delle informazioni relative alla struttura processante impiegata, comprendenti da un lato le informazioni relative alla sfera applicativa degli stessi, ossia quelle relative ai dati e metadati utilizzati come *input* e agli *output* decisionali; dall'altro quelle relative alle caratteristiche tecniche degli algoritmi processati, ossia le informazioni sulle funzionalità sistemiche dell'algoritmo, come il codice sorgente del *software*.

a) Dati personali quali input *dei trattamenti automatizzati*

Per quanto concerne la rilevanza ai fini della disciplina dei segreti commerciali dei dati personali utilizzati come *input* dei sistemi di trattamento automatizzati, è interessante osservare come la medesima direttiva faccia espresso riferimento al considerando n. 2 a "dati commerciali" quali "le informazioni sui clienti"[119].
Il fenomeno dell'utilizzo massiccio di dati personali nelle attività imprenditoriali impone tuttavia un supplemento di riflessione circa la possibile rispondenza dei dati personali ai due requisiti del valore

C. GEIGER (eds.), *Research Handbook on Human Rights and Intellectual Property*, Edward Elgar, 2015, 421 ss..
[117] Cfr. considerando n. 16: "Nell'interesse della innovazione e della concorrenza, le disposizioni della presente direttiva *non dovrebbero creare alcun diritto esclusivo* sul know-how o sulle informazioni che godono di protezione in quanto segreti commerciali". Corsivo aggiunto.
[118] V. FALCE, *Trade Secret Protection in the Innovation Union. From the Italian Approach to the UE Solution,* cit., 24.
[119] J. PILA-P. TORREMANS, European Intellectual Property Law, Oxford University Press, 2016, 538-539;

economico e della non generale o facile accessibilità al dato personale stesso di cui all'art. 2, 1 comma Direttiva UE 943/2016.

In relazione al primo dei suddetti requisiti, è ormai conoscenza acquisita come nella dinamica dei mercati digitali i dati personali abbiano un preziosissimo valore economico, tanto da essere considerati moneta di scambio dei servizi gratuiti ivi offerti[120]. Tuttavia, proprio un'adeguata considerazione del valore economico dell'informazione suggerisce come difficilmente si possa attribuire valore commerciale a un singolo dato personale e che pertanto altrettanto difficilmente lo stesso possa rilevare come segreto[121]. A diverse conclusioni si giunge al contrario se si considera il singolo dato personale come parte di un più ampio giacimento di dati aggregato dall'impresa processante[122]. In questa prospettiva, il requisito del valore economico consente di estendere la tutela della segretezza commerciale anche a "informazioni aziendali" di ultima generazione, come i dati personali dei consumatori nei mercati digitali.

Per quanto concerne invece il requisito della non generale o facile accessibilità dell'informazione segreta, la facile accessibilità dei dati personali parrebbe idonea ad escludere *in apicibus* la sussistenza di questo secondo requisito. È quanto sostenuto da autorevole dottrina[123] sulla base della semplice considerazione che i dati personali rilasciati a un'impresa per accedere a un servizio digitale ben potrebbero essere forniti anche a un'altra impresa. A riguardo è tuttavia necessario osservare come la stessa direttiva faccia riferimento a conoscenze "*generalmente* note o *facilmente* accessibili agli esperti ed agli operatori del settore"[124]. Come ricordato da altra parte della dottrina, la nozione di accessibilità nella sistematica della disciplina

---

[120] Cfr. J. DREXL-R.M. HILTY-L. DESAUNETTES-F. GREINER- D. KIM- H. RICHTER- G. SURBLYTÉ-K. WIEDEMANN, *Data ownership and Access to Data, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*, cit., 3.

[121] J. DREXL-R.M. HILTY-L. DESAUNETTES-F. GREINER- D. KIM- H. RICHTER- G. SURBLYTÉ-K. WIEDEMANN, *Data ownership and Access to Data, Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate,* cit., 7, ove si afferma che "individual data can hardly qualify as trade secrets".

[122] *Ibid*.: "to qualify as a "secret" in the sense of the Directive, trade secrets do not have to be created *ex nihilo*. Freely accessible information can also constitute a part of a trade secret".

[123] J. DREXL, *Designing Competitive Markets for Industrial Data- Between Propertisation and Access*, Max Planck Institute for Innovation and Competition Research Paper n. 16-13, 31 ottobre 2016, reperibile online all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862975, 23 ss..

[124] Cfr. art. 2, 1 comma direttiva UE 943/2016. Corsivo aggiunto.

del segreto commerciale deve interpretarsi in prospettiva relativo-funzionale[125], sì da considerare rilevanti unicamente quelle divulgazioni che risultino idonee a distruggere il valore economico dell'informazione. Posto che il singolo dato personale è parte di un più ampio giacimento di dati aggregato dall'impresa processante[126], può ragionevolmente affermarsi come solo la generale o facile accessibilità dell'intero giacimento di dati possa essere idoneo a pregiudicare il valore economico derivante dal medesimo, e dunque a fare venire meno la segretezza dell'informazione. È esattamente quanto indicato dall'art. 2, 1 comma Direttiva UE 943/2016, ove si precisa come il requisito della segretezza debba riguardare le informazioni commerciali "*nel loro insieme o nella precisa configurazione e combinazione dei loro elementi*"[127]. La disposizione suggerisce dunque come non sono da ritenersi generalmente o facilmente accessibili quelle informazioni che, seppur in parte conosciute da terzi, rappresentano una fonte di vantaggio competitivo per l'impresa che le mantiene riservate nel loro complesso.

b) Dati personali quali output *dei trattamenti automatizzati*

In relazione alla possibilità di tutelare come segreti commerciali i dati personali *generati* dai trattamenti automatizzati e dunque costituenti gli *output* dei medesimi trattamenti nella forma di classificazioni, *scoring*, statistiche, previsioni e correlazioni, occorre muovere qualche considerazione aggiuntiva.
Alla luce della definizione estremamente ampia di segreto commerciale di cui alla Direttiva UE 943/2016, sembra potersi ragionevolmente affermare come anche le informazioni direttamente create dall'algoritmo possano essere oggetto della disciplina in esame[128].

---

[125] È quanto ricorda A. OTTOLIA, *Big Data e innovazione computazionale,* cit., 53.
[126] *Ibid*.: "to qualify as a "secret" in the sense of the Directive, trade secrets do not have to be created *ex nihilo*. Freely accessible information can also constitute a part of a trade secret".
[127] Corsivo aggiunto. Cfr. A. OTTOLIA, *Big Data e innovazione computazionale*, cit., 56 il quale ricorda come alcune pronunce della giurisprudenza di merito abbiano affermato la rilevanza come segreto commerciale degli elenchi della clientela anche di fronte alla possibilità per i concorrenti di conoscere i dati di uno o più clienti. Così Trib. Venezia 16 luglio 2015, in Riv. dir. ind., 2015, 437 e già Trib. Genova 19 giugno 1993, in *GADI*, 1994, 368 ss..
[128] A. OTTOLIA, *Big Data e innovazione computazionale*, cit., 56.

Tale conclusione sembra essere ulteriormente suffragata dal fatto che tali dati generati dai trattamenti automatizzati- pur essendo riferibili a soggetti specifici e pertanto da considerarsi di natura personale ai sensi del Regolamento dati personali[129]- sono prodotti immateriali risultanti in via diretta dall'attività imprenditoriale e dagli investimenti a questa connessi, e dunque degni di appropriazione mediante uno strumento che protegga "l'accesso e lo sfruttamento" del patrimonio conoscitivo dell'impresa[130]. I dati generati dai trattamenti automatizzati sono difatti esattamente il frutto di quegli investimenti sulla produzione che la disciplina in materia di segreti commerciali si prefigge di tutelare "*as such*", senza il requisito aggiuntivo della originalità della creazione richiesto dalla tutela autoriale ovvero quello della organizzazione caratterizzante la tutela delle banche dati. Quest'ultimo strumento attiene difatti ad una successiva attività di organizzazione di un giacimento di dati già originato[131] e può pertanto venire a sovrapporsi, in via eventuale[132], al segreto insistente sui medesimi dati.

c) Dati relativi all'architettura algoritmica

Per quanto concerne le informazioni relative caratteristiche strutturali dei metodi computazionali impiegati, deve innanzitutto osservarsi come queste siano qualificabili alla stregua di "conoscenze tecnologiche" le quali sono espressamente menzionate al considerando n. 2 della direttiva UE 943/2016 quali informazioni meritevoli di riservatezza[133].
La specifica natura delle informazioni in questione impone alcune osservazioni circa l'interazione tra la tutela della riservatezza e la tutela autoriale del software. Questa, come è stato osservato[134], opera come *lex*

---

[129] Il Regolamento fornisce una definizione di dato personale molto ampia, come "qualsiasi informazione riguardante una persona fisica *identificata* o *identificabile*". Cfr. art. 4,1 comma RGDP.

[130] Cfr. considerando n. 1 Direttiva UE 943/2016. Sulla distinzione tra dati personali generati dal soggetto interessato e dati personali generati dall'impresa, si rimandi a G. MALGIERI, *Trade Secrets v. Personal Data: a Possible Solution for Balancing Rights*, in *International Data Privacy Law*, 2016, 6, 2, 102 ss..

[131] Sul punto sia consentito il rinvio a M. BERTANI, *Banche dati e appropriazione delle informazioni*, in *Europa e diritto privato*, 2006, 319 ss..

[132] A. OTTOLIA, *Big Data e innovazione computazionale*, cit., 73 ss..

[133] N. SHEMTOV, *Beyond the Code: Protection of Non-Textual Features of Software*, cit., 220.

[134] G. NOTO LA DIEGA, *Against the Dehumanisation of Decision-Making- Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information*, cit., 11.

specialis rispetto alla *lex generalis* della disciplina in materia di segreti commerciali. La direttiva Software[135] ha ridisegnato la tutela giuridica relativa ai programmi per elaboratore, ridefinendo i confini della stessa tracciati dalla precedente direttiva del 1991[136].

Le persistenti incertezze riguardanti il raggio di tutela accordato ai programmi per elaboratore, avevano già reso necessario l'intervento chiarificatore della Corte di giustizia nella pronuncia *Sas Institute Inc. c. World Programming Ltd.*[137] ove la Corte aveva chiarito come il diritto di software comprenda unicamente "le forme di espressione di un programma per elaboratore e i lavori preparatori di progettazione atti a concludersi, rispettivamente, con la riproduzione o la ulteriore elaborazione di tale programma"[138], ma non "la funzionalità di un programma siffatto né il linguaggio di programmazione e il formato di file di dati utilizzati nell'ambito di un tale programma per sfruttare talune delle sue funzioni"[139]. In questo modo la Corte ha riaffermato il tradizionale principio di diritto per cui il diritto d'autore protegge unicamente la forma espressiva e dunque la componente testuale, e non già il contenuto di un'idea[140]. Estendere la tutela autoriale del software alle idee, comporterebbe, come osservato dall'avvocato generale nella citata pronuncia, una monopolizzazione delle stesse idee "a discapito del progresso tecnico e dello sviluppo industriale"[141].

---

[135] Direttiva 2009/24/CE del Parlamento europeo e del Consiglio del 23 aprile 2009 relativa alla tutela giuridica dei programmi per elaboratore, OJ L 111, 5 Maggio 2009, 16–22 (di seguito Direttiva Software).

[136] Direttiva 91/250/CEE del Consiglio del 14 maggio 1991 relativa alla tutela giuridica dei programmi per elaboratore, OJ L 122 del 17 maggio 1991 42 – 46.

[137] Corte di giustizia, *SAS Institute Inc*, contro *World Programming Ltd.,* Grande Sezione, 2 maggio 2012, C-406/10, reperibile online all'indirizzo http://curia.europa.eu/juris/document/document.jsf?docid=122362&doclang=IT. Per un commento si rimandi alle osservazioni di G. NOTO LA DIEGA, *I programmi per elaboratore e i confini del diritto d'autore. La Corte di giustizia nega la tutela a funzionalità, linguaggio di programmazione e formato dei* file *di dati*, in Rivista di diritto dell'economia, dei trasporti e dell'ambiente, 2013, IX, 69 ss..

[138] Corte di giustizia, *SAS Institute Inc*, contro *World Programming Ltd.,* cit., para 37.

[139] *Ibid*., para 46.

[140] J. LITMAN-P. SAMUELSON, *The Copyright Principles Project: Directions for Reform*, in *Berkeley Technology Law Journal*, 2010, 25, 1175 ss., 1190-1191.

[141] Corte di giustizia, *SAS Institute Inc*, contro *World Programming Ltd.,* cit..

In applicazione del suddetto principio di diritto rientrano nella tutela autoriale del software il codice sorgente e il codice oggetto[142] nella misura in cui siano espressivi del linguaggio informatico con cui il programma è stato elaborato, ma non quanto attiene agli aspetti funzionali del medesimo, come avviene nel caso dell'interfaccia grafica[143].

Il materiale informativo relativo alle proprietà funzionali dei sistemi algoritmici non proteggibile attraverso il diritto di software, trova più sicura protezione in seno alla più ampia tutela del segreto commerciale. Come è stato osservato[144], la tutela autoriale del codice oggetto del software permette all'impresa titolare del diritto di distribuire e dunque di rendere accessibile il software al pubblico, mantenendo però segrete le informazioni relative alle componenti a più alto valore concorrenziale[145]. La protezione autoriale viene così a costituire una forma di tutela insistente sul programma impiegato per il trattamento, di natura aggiuntiva ed eventuale rispetto al segreto.

Il rapporto tra tutela di software e segreto è codificato all'art. 6 della Direttiva Software dove è predisposta una puntuale disciplina dell'utilizzo delle informazioni commerciali riservate conseguite attraverso l'opera di *reverse engineering*. La norma, che consente la decompilazione di un programma al fine di conseguire l'interoperabilità con un altro programma creato autonomamente, vieta al suo secondo comma la comunicazione a terzi delle informazioni acquisite durante l'opera di decomposizione. Un ulteriore divieto è posto in relazione all'utilizzo delle stesse informazioni a fini diversi dal conseguimento della interoperabilità tra programmi e più precisamente al fine dello "sviluppo, la produzione o la

---

[142] Il codice sorgente è definito come "any collection of statements or declarations written in some human readable computer programming language". Così A. MOHAN, *Copyright Issues related to Customized Software*, 1 November 2009, reperibile online all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1497363, 2.

[143] Cfr. Corte di giustizia, C-393/09, *Bezpečnostní softwarová asociace-Svaz softwarové ochrany* contro *Ministerstvo kultury,* 22 dicembre 2010. Per un commento M. BASSINI, *L'interfaccia grafica utente di un software è tutelabile mediante diritto di autore?,* in *Medialaws*, 27 aprile 2011, reperibile online all'indirizzo http://www.medialaws.eu/linterfaccia-grafica-utente-di-un-software-e-tutelabile-mediante-diritto-dautore/.

[144] Segue un medesimo ragionamento E. AREZZO, *Protezione del segreto e tutela del software: convergenze, sovrapposizioni e conflitti*, in *Il diritto industriale*, 2018, 2, 145 ss., 148.

[145] Cfr. anche E. AREZZO-G. GHIDINI, *Dynamic competition in software development. How copyrights and patents, and their overlapping, impact on derivative innovation,* in *Queen Mary Journal of Intellectual Property*, 2013, 3, 4, 278.

commercializzazione di un programma sostanzialmente simile nella sua espressione"[146].
La disposizione in esame sembra dunque predisporre una tutela di natura "rafforzata" delle strutture di processazione algoritmica, coperte nella loro rappresentazione esteriore dal diritto sul software e nel loro contenuto interno dal segreto commerciale. La sovrapposizione delle due tutele finisce per impedire utilizzi di informazioni che sarebbero leciti ai sensi della disciplina dei segreti commerciali: l'art. 6, 2 comma della direttiva software impedisce invero l'utilizzo di informazioni ottenute attraverso attività di decompilazione, diversamente dall'art. 3, 1 comma lett. b della direttiva sui segreti commerciali ai sensi del quale è lecita l'acquisizone, l'utilizzo e la divulgazione di un segreto commerciale attraverso l'"osservazione, studio, smontaggio o prova di un prodotto o di un oggetto messo a disposizione del pubblico (…)". La direttiva software sembra in questo senso ridefinire, estendendoli, i confini della tutela del segreto commerciale, quando a questa si aggiunge il diritto autoriale.

4.2 Il paradigma del segreto sulle informazioni relative al trattamento automatizzato: implicazioni intra- *ed* extra-*sistemiche*

Nell'economia degli algoritmi l'attività delle imprese digitali appare sempre maggiormente incentrata su processi *decisionali* contrapponentisi ai tradizionali processi *produttivi*[147]: questi processi decisionali consistono appunto nello sfruttamento di dati personali raccolti al fine della produzione di altre informazioni nella forma di correlazioni e previsioni che da ultimo orientano l'allocazione di prodotti o servizi offerti.
Dalle considerazioni svolte nei paragrafi precedenti emerge come gran parte delle informazioni che i) alimentano (*input*), ii) afferiscono a e iii) vengono create (*output*) dai sistemi di trattamento automatizzato sono suscettibili di tutela ai sensi della disciplina del segreto commerciale. Dal punto di vista dell'impresa processante, pertanto, la configurazione del segreto commerciale come tracciato dalla riforma appare uno strumento idoneo, in combinazione o meno con altri strumenti di proprietà intellettuale come il diritto sulle banche dati ovvero il diritto d'autore sul

[146] Art. 6, 2 comma Direttiva Software.
[147] Per una ricostruzione in chiave storica delle trasformazioni produttive, si rimandi a G. OLIVIERI, *Dal mercato delle cose al mercato delle idee*, in *Rivista delle società*, 2017, 4, 815 ss..

software, a proteggere le entità immateriali relative alla processazione di dati personali compresi nei beni d'impresa.

La crescente importanza, nei mercati digitali e non solo[148], di strumenti di processazione algoritmica di dati sembra dunque ulteriormente consolidare la centralità della segretezza come paradigma di tutela maggiormente funzionale[149] a proteggere le informazioni aziendali contro i rischi di *free-riding* del pubblico dominio[150].

Il fenomeno in esame ha diretti riflessi sul piano *intra*-sistematico dei diritti di proprietà intellettuale e sul piano *extra*-sistematico, relativo alla interazione dello stesso sistema di diritti di proprietà intellettuale con altre normative, e per quel che in questa sede rileva con la disciplina in materia di dati personali.

Sul piano *intra*-sistemico, la crescente rilevanza di trattamenti automatizzati dei dati personali nell'attività d'impresa sta rafforzando, per ragioni strutturali proprie degli stessi, quelle tendenze di protezionismo informativo che hanno giustificato l'introduzione a livello europeo di nuovi strumenti di tutela dei beni immateriali, come il diritto *sui generis* sulle banche dati, il diritto autoriale sul *software* e, da ultimo in linea storica, il diritto al segreto come armonizzato[151].

Per effetto di questa espansione del sistema dei diritti di proprietà intellettuale[152], lo strumento principe della tutela brevettuale insistente sul prodotto del processo inventivo sembra cedere il passo a nuove forme di

---

[148] Si pensi al crescente impiego di tecniche di *scoring* algoritmico nel settore creditizio,

[149] J. REICHMAN-P. SAMUELSON, *Intellectual Property Rights in Data?,* in *Vanderbilt Law Review*, 1997, 50, 52 ss..

[150] J. BOYLE, *The Second Enclosure Movement and the construction of the Public Domain*, in *Law and Contemporary Problems*, 2003, 66, 33 ss., e più in generale see J. STIGLITZ, *Knowledge as a Public Good,* in I. KAUL- GRUNBERG- M. STERN, *Global Public Goods: International Cooperation in the 21st Century,* Oxford Scholarship Online, 2003, 75 ss.; K.E. MASKUS- J. REICHMAN, *The Globalisation of Private Knowledge Goods and the Provatization of Global Public Goods,* in *Journal of International Economic Law,* 7, 2004, 279 ss., 297.

[151] Malgrado esuli dalla presente trattazione, può ricordarsi nella medesima prospettiva anche l'introduzione del diritto alla c.d. *data exclusivity* di cui all'art.10 direttiva 2001/83/CE.

[152] Sottolinea l'effetto espanisvo delle riforme in materia di proprietà intellettuale già H. ULLRICH, *Expansionist Intellectual Property Protection and Reductionist Competition Rules: a TRIPS Perspective,* in *Journal of International Economic Law,* 7, 2004, 402 ss.

esclusiva riguardanti le conoscenze tecnologiche, quali preziosi momenti del processo decisionale d'impresa[153].

L'evoluzione sopra delineata ha portato alla delineazione di "regimi ibridi"[154] o stratificati[155] di proprietà intellettuale che coprono l'intero ciclo dei processi decisionali e che impediscono in via diretta o indiretta la divulgazione, la riproduzione e la riutilizzazione del *know-how* tecnico.

Nell'assetto così delineato, il segreto commerciale sembra avere non più la sola funzione di *gap-filling* rispetto agli *asset* immateriali posti al di sotto della soglia di brevettabilità[156], ma quella di base protettiva primaria e necessaria delle informazioni tecniche legate al trattamento automatizzato, alla quale in via eventuale e per così dire accessoria si possono sovrapporre il diritto sulle banche dati e la tutela autoriale del *software*.

La centralità della tutela offerta dal segreto commerciale relativamente agli algoritmi industriali ha immediati riflessi sul piano *extra*-sistemico, ossia sulla interazione "orizzontale"[157] della tutela del segreto con altri diritti di senso contrario e postulanti la trasparenza delle informazioni relative alle tecnologie processanti.

La tensione tra segreto e diritti di accesso all'informazione[158] non è certo nuova ed è tradizionalmente emersa in relazione a varie tipologie di informazioni, quali i dati farmaceutici[159], le informazioni ambientali[160],

---

153 Per un'analisi più approfondita di tale evoluzione sia consentito il rimando a G. SCHNEIDER, *European Intellectual Property and Data Protection in the Digital Algorithmic-Economy: a Role Reversal (?),* in *Journal of Intellectual Property Law and Practice*, 2018, 13, 229.

154 H. ULLRICH, *Expansionist Intellectual Property Protection and Reductionist Competition Rules: a TRIPS Perspective,* cit., 412 ss..

155 Si veda, in generale, E. DERCLAYE, *Overlapping Rights*, in R. DREYFUSS- J. PILA, *The Oxford Handbook of Intellectual Property Rights*, 2017, reperibile online all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930841, *passim*.

156 H. ULLRICH, *Expansionist Intellectual Property Protection and Reductionist Competition Rules: a TRIPS Perspective,* cit., 412 ss..

157 A. OTTOLIA, *Big Data e innovazione computazionale*, cit., 153.

158 M.L. LYNDON, *Secrecy and access in an innovation intensive economy: reordering information privileges in environmental, health, and safety law,* in *University of Colorado Law Review*, 2007, 78, 466.

159 G. SCHNEIDER, *A European Transparency Challenge: can commercial confidentiality over clinical trials be overcome?*, in *European Pharmaceutical Law Review*, 2018, 2, 1, 3 ss..d

160 P.H. SAND, *The Right to Know: Environmental Information disclosure by Government and Industry,* 2002, reperibile online all'indirizzo https://www.researchgate.net/publication/228464480_The_Right_to_Know_Environmental_Information_Disclosure_by_Government_and_Industry.

finanziarie[161], i documenti amministrativi[162], e non da ultimo i dati personali.
Il conflitto tra diritti di accesso e diritti di segretezza sembra tuttavia destinato ad inasprirsi in conseguenza della evoluzione da un lato della disciplina in materia di dati personali verso istanze di maggiore trasparenza dei metodi automatizzati di processazione di dati personali, dall'altro della disciplina in materia di segreto commerciale verso un ampliamento del suo raggio applicativo in relazione agli stessi trattamenti algoritmici.
Il rilascio delle informazioni relative al trattamento automatizzato potrebbe infatti recare pregiudizio alle imprese facenti impiego di tecnologie algoritmiche da più prospettive: non solo infatti imprese concorrenti potrebbero sfruttare il *know-how* tecnico a propri fini, dissolvendo il vantaggio competitivo conquistato dall'impresa titolare del segreto, ma il rilascio, ad esempio, dei criteri di categorizzazione ovvero dei criteri predittivi impiegati potrebbe causare un pregiudizio reputazionale alla stessa impresa processante qualora tali criteri si rivelino discriminatori. Ancora, la conoscenza dei meccanismi di funzionamento dei trattamenti automatizzati potrebbe facilitare pratiche di c.d. *gaming* degli stessi algoritmi processanti[163].

5. Il bilanciamento tra diritti di verificabilità e diritto alla segretezza algoritmica: le soluzioni della giurisprudenza

Il contrasto tra diritto alla segretezza e le istanze di accesso a dati relativi ai trattamenti di dati personali è stato oggetto di alcune pronunce giurisprudenziali nazionali che sotto il regime della precedente direttiva hanno fortemente limitato il diritto di accesso ai dati personali già codificato all'art. 12 Diretta 95/46/CE[164].
In alcuni ordinamenti, come quello inglese, la tutela del segreto commerciale costituisce una vera e propria eccezione al diritto di accesso

[161] Cfr. B. REDDIX-SMALLS, *Credit Scoring and Trade Secrecy: an Algorithmic Quagmire or How the Lack of Transparency in Complex Financial Models Scuttled the Financial Market*, in *UC Davis School of Law Business Law Journal*, 2011, 12, 87, 117-118.
[162] E. KORKEA-A. LENO, *Who owns information held by EU Agencies? Weed killers, Commercially sensitive information and participatory governance*, in *Common Market Law Review*, 2017, 54, 1059 ss..
[163] J.R. BAMBAUER-T.ZARSKY, *The Algorithm Game*, in *Notre Dame Law Review*, 2018, 94,1 ss..
[164] S. WACHTER- B. MITTELSTANDT- L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making does not exist in the General Data Protection Regulation*, cit., 85.

del soggetto interessato alla logica applicata ai trattamenti automatizzati[165]. Tale eccezione è stata interpretata in modo molto ampio dalla dottrina e dalle corti inglesi, che hanno inteso limitare il diritto di accesso dell'interessato al fine di tutelare il segreto commerciale sulle informazioni relative al sistema di processazione dei dati non solo da parte dell'impresa titolare del trattamento, ma anche da parte dell'impresa fornitrice dello stesso sistema[166]. Un approccio simile è stato seguito nell'ordinamento francese[167] e in quello tedesco.

Qui una pronuncia del *Bundesgerichtshof* ha affrontato la specifica questione dell'incidenza della tutela del segreto sul diritto di accesso alla logica del trattamento automatizzato in relazione a un sistema di *scoring* sulla affidabilità creditizia[168]. La richiesta di un soggetto interessato di accedere alle informazioni relative alla logica del sistema di *scoring* e dunque alle informazioni sui metodi della valutazione dell'affidabilità creditizia, è stata da ultimo respinta dalla Corte federale tedesca. I giudici tedeschi hanno affermato come il diritto di accesso alla logica utilizzata dal trattamento automatizzato debba essere interpretato nel senso da comprendere unicamente i dati personali che sono stati rilevanti ai fini del trattamento (*input*) e della decisione conseguente (*output*), ma non le formule di *scoring*, i dati statistici e le informazioni relative ai *cluster* di riferimento[169].

Un orientamento opposto è stato recentemente espresso dalla giurisprudenza amministrativa italiana, relativamente alla richiesta di accesso alle informazioni sulle proprietà funzionali di una procedura automatizzata utilizzata dal ministero dell'istruzione per il trasferimento interprovinciale dei docenti scolastici[170]. In questa occasione, il Tar Lazio ha precisato come i diritti di proprietà intellettuale insistenti sull'algoritmo non ostano alla riproduzione, nella forma della visione e dell'estrazione della copia da parte del soggetto interessato, di informazioni sulla logica del "test" algoritmico, fintantoché la stessa riproduzione non comporti uno sfruttamento economico delle medesime informazioni. Come sostenuto dal

---

[165] Cfr. United Kingdom Data Protection Act del 1998, Sezione 7 (1) e sezione 8(5).

[166] Per una analisi della giurisprudenza inglese, P. COPPEL, *Information Rights: Law and Practice*, Oxford-Portland-Oregon, Hart Publishing, 2014, 150.

[167] Cfr. art. 39, 1 comma, 5, della *Loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, come riformato nel 2004.

[168] *Bundesgerichtshof*, 28 gennaio 2014, VI ZR, 156/13, c.d. pronuncia "Schufa".

[169] *Ibid*., para 39-40.

[170] Tar Roma, Sez. III del 21 marzo 2017 n. 3742,

giudice amministrativo, infatti, la disciplina in materia di diritti di proprietà intellettuale mira alla tutela di interessi di natura economica dei relativi titolari[171], i quali non sarebbero pregiudicati dall'accesso alle medesime informazioni demandato da un'altra disciplina posta a tutela di interessi di natura radicalmente differente, in specie interessi legittimi[172].
In questi termini, il Tar Lazio propone un approccio sistematico alla delimitazione dei diritti di proprietà intellettuale[173] rispetto all'ambito di applicazione di altre normative, non oltre quanto sia *proporzionalmente* necessario a garantire una piena protezione degli interessi sottesi alla relativa disciplina.
La pronuncia in esame sembra dunque implicitamente applicare il principio di proporzionalità all'operazione di bilanciamento tra diritti fondamentali, sulla scorta dell'insegnamento della Corte di giustizia nel noto caso *Promusicae*[174]. L'importanza del principio di proporzionalità quale parametro fondamentale nell'operazione di bilanciamento[175] tra diritti di proprietà intellettuale e il diritto al rispetto della vita privata è stata riaffermata in una recentissima pronuncia della stessa Corte di Giustizia, che ha precisato come le limitazioni ai diritti e alle libertà riconosciuti dalla Carta di Nizza devono rispettare "il contenuto essenziale di detti diritti e libertà"[176].
Secondo posizioni simili a quelle espresse dal Tar Lazio, la Corte di giustizia ha preso in esame il contrasto tra diritto di accesso a informazioni commerciali e diritto alla segretezza nel settore farmaceutico, chiarendo

---

[171] Riflette sul punto V. FALCE, *Accesso all'algoritmo e segreto industriale, che dice la giurisprudenza italiana*, 26 Aprile 2018, reperibile online all'indirizzo https://www.agendadigitale.eu/mercati-digitali/accesso-allalgoritmo-e-segreto-industriale-che-dice-la-giurisprudenza-in-italia/.
[172] Il caso concerneva difatti la richiesta di accesso alle informazioni sul funzionamento dell'algoritmo non già sotto la disciplina in materia di dati personali, bensì in materia di accesso agli atti amministrativi di cui all'art.22 l. 241/1990.
[173] V. FALCE, *Accesso all'algoritmo e segreto industriale, che dice la giurisprudenza italiana,* cit..
[174] Corte di Giustizia dell'Unione europea, C-275/06, *Promusicae*. La pronuncia ha ad oggetto il conflitto tra diritto al rispetto della vita privata e altri diritti, tra cui quello di proprietà.
[175] Per una più approfondita analisi del c.d.test di proporzionalità elaborato dalla Corte di Giustizia, si rimani a G. ALPA- G. RESTA, *Le persone e la famiglia, vol 1: Le persone fisiche e i diritti della personalità,* in R. SACCO (a cura di), *Trattato di diritto civile*, Assago, Utet giuridica, 2006, 588. Cfr. anche C.B. TRANBERG, *Proportionality and Data Protection in the Case law of the European Court of Justice*, in *International Data Privacy Law*, 2011,4,1, 239 ss..
[176] Corte di giustizia dell'Unione europea, C-149/17, *Bastei Lübbe GmbH & Co.KG contro Michael Strotzer*, 18 ottobre 2018.

come il segreto commerciale su informazioni relative a prodotti farmaceutici può essere idoneo a limitare il diritto di accesso unicamente in presenza di un "rischio grave e irreparabile" agli interessi commerciali dell'impresa[177].
Un'interpretazione di natura "funzionale" della tutela del segreto, valorizzata nella sua *ratio* primaria di tutela degli incentivi all'innovazione[178], è stata proposta anche da una parte della dottrina che ha sottolineato la opportunità di limitare il raggio di protezione offerto dal segreto ai soli utilizzi delle informazioni commerciali riferibili all'attività principale e attuale dell'impresa titolare[179]. Seguendo questo ragionamento, il rilascio di informazioni sul trattamento automatizzato al singolo individuo interessato ovvero ad un'impresa operante in un settore economico diverso non sarebbe pertanto idoneo a pregiudicare la competitività dell'impresa titolare e dunque a vanificare la tutela del segreto commerciale.

5.1. La soluzione interpretativa: verso una ricomposizione del mosaico normativo

Il riferimento alla tutela del segreto e del *software* contenuto al considerando n. 63 RGDP[180] costituisce un elemento interpretativo utile ai fini della lettura dell'art. 23 RGDP, ove è precisato come i diritti di notifica e di accesso possono essere limitati dal diritto dell'Unione o dello stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento, "qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali, e sia una misura necessaria e proporzionata" per salvaguardare, *inter alia,* "i diritti e le libertà altrui", quali ad esempio i diritti di proprietà intellettuale dell'impresa titolare del trattamento.

---

[177] Corte di Giustizia dell'Unione europea, C-390/13, *Agenzia europea per i medicinali (EMA) contro Intermune* e C-389/13, *Agenzia europea per i medicinali (EMA) contro Abbvie.* Le due pronunce ha ad oggetto la richiesta di accesso ai documenti dell'agenzia del farmaco sotto il Regolamento CE n. 1049/2001.
[178] Cfr. il considerando n. 1 della direttiva UE 943/2016.
[179] J. DREXL, *Designing Competitive Markets*, cit., 24.
[180] Considerando n. 63 RGDP: "(…) ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto 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 (…)."

Pur ammettendo una limitazione ai diritti di trasparenza, la norma riafferma la necessità che tale limitazione avvenga in via proporzionale a quanto strettamente necessario alla tutela dell'interesse che giustifica la limitazione medesima. In questa prospettiva, è lo stesso considerando n. 63 RGDP che precisa come la tutela del segreto o del software non dovrebbe "*condurre a un diniego a fornire all'interessato tutte le informazioni*"[181].
Il Regolamento dati personali sembra dunque affermare, seppur a livello di considerando e non di disposizione ad efficacia vincolante, la non derogabilità *in toto* del principio di trasparenza relativo al trattamento dei dati personali e pertanto la necessaria prevalenza dei relativi diritti del singolo individuo rispetto alle rivendicazioni delle imprese.
In altri termini, ai sensi del Regolamento dati personali, l'erosione delle previsioni sulla trasparenza algoritmica per effetto del segreto commerciale incontra il limite della necessità di garantire l'effettività dei diritti alla trasparenza riconosciuti al singolo. Tale limite deve essere indubbiamente identificato in base al parametro di proporzionalità, e in base alla considerazione della *ratio* più profonda sottesa alle disposizioni in materia di trasparenza algoritmica, come funzionali alla salvaguardia della libertà di autodeterminazione del singolo nella dimensione digitale[182].
Dalla prospettiva opposta, anche la direttiva sul segreto commerciale contiene alcune previsioni di bilanciamento con l'interesse alla protezione dei dati personali: i considerando n. 34 e 35 RGDP affermano espressamente come la direttiva in materia di segreto "rispetta i diritti fondamentali e osserva i principi riconosciuti in particolare dalla Carta, nella fattispecie (…) il diritto alla protezione dei dati personali" e pertanto "non dovrebbe pregiudicare i diritti e gli obblighi stabiliti dalla direttiva 95/46/CE, in particolare i diritti della persona interessata di accedere ai suoi dati personali che sono oggetto di trattamento (…)"[183]. La stessa direttiva, inoltre codifica alcune ipotesi di acquisizione, utilizzo e divulgazione leciti dei segreti commerciali all'art. 3 della Direttiva UE 943/2016, che al suo

[181] *Ibid*., corsivo aggiunto.
[182] Per la connessione tra privacy e autodeterminazione, si rimandi diffusamente ai rilievi della Corte europea di giustizia nella pronuncia *Digital Rights Ireland and Seitlinger and others,* Case C-293/12 and C-594/12, richiamati da A. SPINA, *Risk Regulation of Big Data: Has the time arrived for a Paradigm shift in Eu Data Protection Law?, Case notes to Case C-293/12 and C-594/12* Digital Rights Ireland and Seitlinger and others, in *European Journal of Risk Regulation*, 2014, 5, 2, 248 ss..
[183] Così considerando n. 35 Direttiva UE 943/2016.

secondo comma dichiara lecite le divulgazioni richieste o autorizzate dal diritto dell'Unione. Rafforza ulteriormente tale previsione, l'eccezione di cui al successivo art. 5 lett a) che, ancora, consente la disapplicazione degli strumenti di tutela di cui alla direttiva qualora la "presunta acquisizione, il presunto utilizzo o la presunta divulgazione del segreto commerciale siano avvenuti (…) nell'esercizio del diritto *alla libertà di espressione e d'informazione* come previsto dalla Carta"[184].

Il mosaico normativo così configurato sembra dunque da ultimo riportare alla questione di fondo relativa al bilanciamento tra diritti fondamentali, demandato dall'art. 52 della Carta dei diritti fondamentali dell'Unione europea[185]: da un lato il diritto alla protezione dei dati personali[186] nella sua nuova connessione con il diritto all'informazione[187] e all'autodeterminazione del singolo individuo[188], dall'altro la libertà di impresa[189] e il diritto di proprietà, in seno al quale viene ricondotto il diritto di proprietà intellettuale[190].

Trattandosi nel primo caso di diritti individuali e nel secondo di diritti di natura economica- dunque di diritti aventi diversa dislocazione

---

[184] Corsivo aggiunto.

[185] Art. 52, 1 comma Carta dei diritti fondamentali dell'Unione Europea: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

[186] Art. 8 Carta dei diritti fondamentali dell'Unione Europea, rubricato "protezione dei dati di carattere personale". Cfr. G. GONZÁLES FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU law*, Cham, Springer International, 16, 2014, 204.

[187] Art. 11 Carta dei diritti fondamentali dell'Unione Europea, rubricato "libertà di espressione e d'informazione".

[188] Il principio di autodeterminazione è da ultimo connesso al diritto fondamentale alla dignità umana di cui all'art. 1 della stessa Carta.

[189] Art. 16 Carta dei diritti fondamentali dell'Unione Europea.

[190] Art. 17, 2 comma Carta dei diritti fondamentali dell'Unione Europea. Sulla dibattuta questione se il diritto al segreto commerciale sia tutelabile come dirittto di proprietà intellettuale ai sensi dell'art. 17, 2 comma della Carta si rimandi a M. BRONCKERS-N. MCNEILS, *Is the EU obliged to improve the Protection of Trade Secrets? An Inquiry into TRIPS, the European Convention of Human Rights and the EU Charter of Human Rights*, in *European Intellectual Property Review*, 2012, 10, 673 ss., 680-682, ove gli Autori si esprimono in senso affermativo.

gerarchica[191]-, il bilanciamento, seppur nel rispetto delle complessità delle singole controversie, dovrà necessariamente risolversi a favore dei primi[192].

5.2. La soluzione operativa: la tutela "modulata" del segreto commerciale

L'analisi sin qui tracciata ha messo in luce una più decisa presa di campo di istanze di trasparenza in seno alla disciplina europea in materia di dati personali come riformata dal Regolamento generale dati personali. Come sopra dimostrato, il principio di trasparenza definito dal Regolamento è strettamente connesso a istanze di responsabilizzazione delle imprese facenti impiego di trattamenti automatizzati di dati personali. Questo spiega non solo la molteplicità delle previsioni in materia di trasparenza di cui hanno dato conto i precedenti paragrafi ma anche l'eterogeneità delle medesime.
In questo senso, il Regolamento generale dati personali ha codificato un nuovo diritto dei soggetti interessati del trattamento automatizzato a ottenere una spiegazione dei processi decisionali che lo riguardano. Una più attenta analisi della disciplina in materia di dati personali rivela tuttavia come gli obiettivi della trasparenza algoritmica del Regolamento vadano ben oltre la configurazione di un diritto del soggetto interessato alla spiegazione, e investano in modo più profondo gli assetti organizzativi delle imprese processanti.
Nella sistematica del Regolamento, infatti, la trasparenza dei trattamenti dei dati personali si configura come verificabilità delle strutture algoritmiche processanti, rispettivamente i) da parte dei singoli soggetti

---

[191] Cfr. S. GUTWIRTH, *Privacy and the Information Age*, Lanham, Rowman & Littlefield Publishers, 2002, 46.

[192] V. FALCE, *Accesso all'algoritmo e segreto industriale, che dice la giurisprudenza italiana,* cit.. È la conclusione anche dello European Data Protection Supervisor. Cfr. European Data Protection Supervisor, *Opinion on the Proposal of a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, 12 Marzo 2014, reperibile online all'indirizzo https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf, 5, ove si afferma apoditticamente che "the proposed directive should not interfere with data subjects' rights". Significativa anche la proposta dello stesso Supervisor di un coinvolgimento dei garanti privacy nelle controversie relative al conflitto tra protezione del segreto e del diritto di accesso del soggetto interessato ai dati personali impiegati nel trattamento: "in the event that a conflict arises between the right to protection of trade secrets and the right to access to personal data being processed, it may be advisable to provide for an adjudication process involving the relevant supervisory authorities, including the national data protection authority".

interessati (diritto alla spiegazione) *ex* artt. 13-15 RGDP; ii) da parte delle autorità di controllo *ex* art. 58 RGDP; iii) da parte delle stesse imprese processanti o società terze *ex* art. 35 RGDP.
Come messo in luce, le disposizioni sulla trasparenza algoritmica si distinguono tra di loro per avere ad oggetto diverse tipologie di informazioni: secondo l'interpretazione qui proposta, il diritto alla spiegazione ha ad oggetto unicamente informazioni relative all'impiego concreto dei dati nella singola operazione di trattamento, dunque i dati rilevanti per il trattamento (*input*) e i criteri di classificazione e predittivi (*output*); mentre l'obbligo di valutazione d'impatto e i poteri di indagine da parte dell'autorità di controllo hanno ad oggetto informazioni a più alto contenuto tecnico relative al funzionamento delle strutture processanti, intellegibili unicamente da parte di esperti.
Lungi dall'avere valenza meramente descrittiva, la categorizzazione qui proposta delle disposizioni sulla verificabilità algoritmica risulta rilevante in relazione alla definizione dei limiti giuridici alla stessa verificabilità tracciati dalla disciplina del segreto commerciale. A ben guardare, infatti, poiché ciascuna delle tre categorie di disposizioni sulla trasparenza algoritmica ha ad oggetto diverse informazioni relative ai trattamenti algoritmici ed è funzionale alla protezione di interessi diversi, ciascuna interagisce diversamente con la tutela del segreto.
In base al quadro normativo di riferimento, in relazione alle informazioni relative ai trattamenti automatizzati, la tutela del segreto sembra doversi atteggiare in una forma "modulata", secondo quanto di seguito illustrato.

a) *Interazione tra diritto alla spiegazione* ex *artt. 13-15 RGDP e segreto:*

Il diritto alla spiegazione si configura come il diritto del singolo soggetto interessato a ricevere da parte dell'impresa titolare del trattamento *ex* artt. 13 e 14 RGDP ovvero ad accedere *ex* art. 15 RGDP a informazioni "significative" sulla logica del trattamento automatizzato impiegato. Come sopra esposto, il diritto riguarda unicamente quelle informazioni relative agli *input* e gli *output* dei trattamenti automatizzati che il soggetto interessato è in grado di comprendere, sì da renderlo in grado di azionare altri diritti contenuti nel Regolamento, quali il diritto all'oblio o il diritto alla portabilità dei dati. La *ratio* ultima è dunque quella di mitigare le asimmetrie informative tra imprese processanti i dati e soggetti interessati,

tutelando così il diritto degli stessi a autodeterminarsi nelle dinamiche dei mercati digitali. In questa prospettiva, la tutela del segreto relativo alle informazioni sugli *input* e gli *output* dei trattamenti automatizzati non appare idonea a restringere il materiale informativo di cui il Regolamento richiede il rilascio non solo per la preminenza dei diritti fondamentali individuali rispetto a diritti di natura economica[193], ma anche perché il rilascio di tali informazioni ai singoli individui- e non già a imprese concorrenti- non sembra in alcun modo idonea a pregiudicare il vantaggio competitivo dell'impresa processante[194].

b) Interazione tra potere di verifica dell'autorità di controllo ex *art. 58 RGDP e segreto:*

Diverse considerazioni devono svolgersi in relazione al potere di revisione dei trattamenti automatici posto in capo all'autorità di controllo. Secondo la ricostruzione qui proposta, tale potere ha ad oggetto informazioni strutturali, a contenuto tecnico altamente sofisticato, sul funzionamento delle strutture processanti. L'art. 58 RGDP assegna infatti alle stesse autorità di controllo il compito di verificare la correttezza della progettazione degli algoritmi processanti al fine di monitorare la liceità e la correttezza dei trattamenti medesimi e di rilevare dunque eventuali schemi computazionali discriminatori[195]. In questo senso, il potere investigativo delle autorità di controllo ha ad oggetto informazioni commerciali estremamente confidenziali, giacché costituenti il nucleo per così dire duro del *know-how* di carattere tecnico dell'impresa.
Come nel caso precedente, tuttavia, anche in questo caso la *disclosure* di tali informazioni non è idonea a pregiudicare gli investimenti in innovazione dell'impresa processante, posto che il destinatario della medesima *disclosure* è non un soggetto privato bensì una pubblica autorità[196]. A riguardo, è la stessa Direttiva UE 943/2015 a precisare come la disciplina in materia di segreto commerciale "non dovrebbe pregiudicare l'applicazione delle norme dell'Unione o nazionali che prevedono la divulgazione di

[193] A. OTTOLIA, *Big Data e innovazione computazionale,* cit., 177-178 con particolare riferimento alle nota n. 8.
[194] J. DREXL, *Designing Competitive Markets*, cit., 24 ss..
[195] P. HACKER, *Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Decision Making in the EU Law,* cit., 1143 ss..
[196] Considerando n. 11 Direttiva UE 943/2016.

informazioni, inclusi i segreti commerciali al pubblico o *alle autorità pubbliche di raccogliere le informazioni per lo svolgimento dei loro compiti (…)*"[197]. L'accesso alle informazioni relative alla processazione algoritmica è necessario per lo svolgimento dei compiti di revisione sui trattamenti algoritmici deferiti dal Regolamento alle autorità di controllo. In questi termini, l'acquisizione da parte delle stesse autorità sarebbe certamente da considerarsi lecita, fatti salvi "gli obblighi di riservatezza cui (le stesse autorità) sono soggette in relazione alle informazioni trasmesse dai detentori di segreti commerciali, a prescindere dal fatto che tali obblighi siano sanciti dal diritto dell'Unione o da quello nazionale"[198].

c) *Interazione tra obbligo di verifica delle imprese* ex *art. 35 RGDP e segreto:*

Per quanto concerne, da ultimo, l'obbligo della valutazione sull'impatto dei trattamenti effettuati di cui all'art. 35 RGDP, è stato sopra precisato come questo si riferisca principalmente all'identificazione di quelle proprietà strutturali e funzionali dei metodi di processazione algoritmici. Problemi di tutela del segreto commerciale sono destinati a emergere a riguardo specificamente in caso di *auditing* esterno, affidato a imprese terze esperte. In tal caso, ragioni di protezione delle informazioni commerciali ben potrebbero fondare il rifiuto dell'impresa soggetta alla valutazione d'impatto di rilasciare all'impresa terza alcune informazioni costituenti prezioso *know-how* tecnico, impedendo così una valutazione d'impatto approfondita ovvero completa. Posto che si tratterebbe in tal caso di un trasferimento di informazioni non a soggetti individuali o a soggetti pubblici, bensì ad altre imprese, potrebbero ritenersi sussistenti in tal caso le ragioni di tutela del segreto commerciale.
Stando alle posizioni dottrinarie più rigorose, rischi di pregiudizi concorrenziali non dovrebbero emergere in relazione a imprese conducenti attività in settori diversi rispetto a quelli in cui operano i titolari del segreto[199]. Tuttavia, anche a voler ritenere sussistente un simile rischio, questo ben potrebbe essere scongiurato mediante la stipula di accordi di *non-disclosure* con le imprese terze. Lo strumento degli accordi di

[197] Corsivo aggiunto.
[198] Considerando n. 18 Direttiva UE 943/2016.
[199] J. DREXL, *Designing Competitive Markets*, cit., 24.

confidenzialità, e la relativa tutela dei rimedi contrattuali, potrebbe essere dunque valorizzato come strumento utile al rilascio di informazioni commercialmente sensibili sui trattamenti automatizzati di dati personali senza tuttavia far perdere, malgrado il rilascio, alle stesse informazioni lo status di segreto, e alle imprese titolari il vantaggio concorrenziale conquistato[200].

6. Conclusioni

Il presente contributo ha inteso tracciare le linee di evoluzione di due discipline recentemente divenute importanti fonti di regolamentazione delle attività imprenditoriali che si avvalgono delle tecnologie algoritmiche per la processazione di dati personali. La crescente rilevanza economica dei dati[201] ha reso impellente l'intervento del legislatore europeo per rispondere alle sfide poste dall'intelligenza artificiale nel mercato unico digitale, con il duplice obiettivo di preservare gli incentivi all'innovazione e di tutelare al contempo i diritti fondamentali dei consumatori potenzialmente pregiudicati dal massiccio trattamento dei loro dati personali[202].
In questa prospettiva il contributo ha innanzitutto definito i caratteri della trasparenza algoritmica demandata dal Regolamento in materia di dati personali, dimostrando come la stessa non si risolva nel diritto di accesso del singolo soggetto interessato ai dati trattati, ma comprenda strumenti di vera e propria "verificazione" delle strutture processanti, che si traducono in obblighi di valutazione d'impatto gravanti sulle imprese e in veri e propri poteri di revisione posti in capo all'autorità di controllo.
A partire da questa più ampia nozione di "verificabilità" dei trattamenti automatizzati come desumibile dalla sistematica del Regolamento, l'analisi

---

[200] Cfr. A. PORTUESE, From Non-disclosure Agreements to Trade Secrets: Antitrust Implications, in European Competition Law Review, 2018, 39, 274 ss..
[201] Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni- Verso uno spazio comune europeo dei dati*, 25 aprile 2018, reperibile online all'indirizzo https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2018:0232:FIN.
[202] Questa duplice prospettiva è ben messa in luce dalla Commissione europea in una recente comunicazione. Cfr. COMMISSIONE EUROPEA, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions- Artificial Intelligence for Europe*, 25 aprile 2018, reperibile online all'indirizzo https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe.

ha indagato i limiti giuridici alla stessa verificabilità algoritmica segnati dalla limitrofa disciplina del segreto commerciale. Come dimostrato, difatti, la direttiva in materia di segreti commerciali- e l'ampia nozione di segreto qui data- fornisce adeguato fondamento giuridico alle rivendicazioni delle imprese processanti sulle varie componenti informative del ciclo di processazione algoritmica di dati.

Dal quadro così definito, il saggio ha analizzato l'impatto della tutela del segreto sulla verificabilità algoritmica alla luce delle tre diverse categorie di previsioni sulla trasparenza contenute nel Regolamento. In questo modo si è messo in evidenza la necessità di configurare una tutela modulata del segreto relativo al trattamento automatizzato di dati personali, tale da consentire ai soggetti interessati di essere adeguatamente edotti sui trattamenti riguardanti gli stessi; alle autorità di controllo di esercitare i propri poteri di revisione; e alle società terze di condurre valutazioni d'impatto sufficientemente approfondite.

Una simile lettura "orizzontale" della disciplina del segreto appare indispensabile al fine di un perseguimento effettivo degli obiettivi di verificabilità delle strutture processanti che il Regolamento in materia di dati personali si pone. Come suggerito dalla stessa Commissione europea, la verificabilità tecnologica è da considerarsi il punto di partenza nel più ampio progetto di costruzione della fiducia digitale, quale presupposto essenziale per uno sviluppo sostenibile dell'economia dei dati[203]. In questi termini, meglio si comprende come, nella ricostruzione qui proposta, i diritti economici della libertà d'impresa e della proprietà intellettuale arretrano solo in apparenza rispetto al diritto fondamentale della protezione dei dati.

---

[203] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni- Verso uno spazio comune europeo dei dati,* cit., 1.