

## CAPITOLO I

# IL TRATTAMENTO DEI DATI COME ATTIVITÀ DI FLUSSO A DIMENSIONE GLOBALE. PROBLEMI E MODELLI DI TUTELA

SOMMARIO: 1. La dimensione globale del trattamento dei dati e la sua intrinseca cifra/natura di attività *di massa*. – 2. La necessità di un approccio giuridico transnazionale e il ruolo della comparazione. – 3. Dal problema della riservatezza al problema della circolazione dei dati. Verso il superamento della dimensione individuale della tutela giuridica. – 4. Il rischio di illecito trattamento dei dati personali come rischio endemico strutturale. Tipologie di rischio e violazione sistematica dei diritti fondamentali della persona. – 5. Possibili modelli di regolazione e di responsabilità dei titolari in un contesto fortemente asimmetrico. Metodologie di *governance* dei sistemi digitali. – 5.1. Il *public enforcement* e il sistema europeo delle Autorità Indipendenti. – 5.2. I limiti dell'approccio individuale basato sul consenso e sui diritti degli interessati. Potere negoziale e "intermediari dei dati". – 5.3. Il *private enforcement* e la *privacy* di gruppo. – 6. La crisi della giustizia civile nella società di massa e il modello della tutela collettiva. – 7. Lezioni americane: la *privacy litigation*.

### 1. *La dimensione globale del trattamento dei dati e la sua intrinseca cifra/natura di attività di massa*

Una sintesi suggestiva del concetto di identità nell'*infosfera*<sup>1</sup> può essere effettuata prendendo in prestito le parole dello scrittore Ian Mc Ewan, che osserva: "l'io è un racconto incessantemente riscritto"<sup>2</sup>.

---

<sup>1</sup> L. FLORIDI, *Il verde e il blu. Idee ingenue per migliorare la politica*, Milano, 2020, p. 43.

<sup>2</sup> I. MC EWAN, *Il mio romanzo viola profumato*, Torino, 2018, p. 30. L'espressione è, in realtà, attribuita dallo stesso Mc Ewan a J. BRUNER, *The remembered self*, in U. Neisser, R. Vifush (a cura di), *The Remembering Self: Construction and Accuracy in the Self-narrative*, Cambridge, 1994.

Nel mondo della rete, la circolazione dei dati personali, attributi immateriali degli individui, è particolarmente veloce; ogni utente dissemina tracce di sé nel *web*, e delinea e ridisegna costantemente la propria identità digitale, anche senza averne pienamente consapevolezza<sup>3</sup>. Non a caso, “capitalismo informazionale”<sup>4</sup> è una delle espressioni con cui si indica il modello economico della rivoluzione digitale, in cui il controllo delle informazioni consente di influenzare la politica e l’economia<sup>5</sup>. Le tecnologie integrate che permettono l’interazione in tempo reale tra soggetti che si trovano in ogni parte del mondo funzionano attraverso lo scambio, l’aggregazione e l’analisi di enormi quantità di dati<sup>6</sup>. Nel-

---

<sup>3</sup> A. QUARTA, G. SMORTO, *Diritto privato dei mercati digitali*, Firenze, 2020, pp. 5-10. Sull’identità digitale si rinvia, per tutti, alle considerazioni di G. ALPA, *L’identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, pp. 723-727.

<sup>4</sup> G. RESTA, *Contratto e diritti fondamentali*, in *Enc. dir., I tematici: Contratto*, Milano, 2021, p. 304 che fa propria l’espressione di J. COHEN, *Between truth and power: the legal constructions of informational capitalism*, Oxford, 2019. “Capitalismo informazionale” è nozione differente e, secondo Resta, più convincente, dal “capitalismo della sorveglianza” (quest’ultima elaborata da S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell’umanità nell’era dei nuovi poteri*, Roma, 2019). Zuboff descrive il capitalismo della sorveglianza come un modello economico in cui la sfera privata dei singoli viene convertita in materia prima dagli attori del mercato, attraverso l’utilizzo delle informazioni personali per migliorare prodotti e servizi, ma soprattutto per effettuare predizioni comportamentali. Tali predizioni vengono poi utilizzate in quasi tutti i servizi *online*, commerciali e non. Il capitalismo informazionale di Cohen, invece, recepisce gli spunti di Zuboff, ma tiene conto del ruolo che i formanti del diritto hanno ricoperto nel delineare il modello sociale ed economico in cui oggi ci si trova, in cui i dati rappresentano “una risorsa primaria per qualsiasi attività produttiva e gli stessi modelli di consumo stratificatisi nella società esaltano ed amplificano tale artificiale equiparazione dei dati a *commodities*”. Altra espressione suggestiva per esprimere concetti simili è “capitalismo immateriale”, usata da S. QUINTARELLI, *Capitalismo immateriale. Le tecnologie digitali e il nuovo conflitto sociale*, Torino, 2019.

<sup>5</sup> In merito G. GIANNONE CODIGLIONE, V. ZENO-ZENCOVICH, *Ten legal perspectives on the “big data revolution”*, in *Conc. e mer.*, 2017, pp. 29-30.

<sup>6</sup> È il modello dell’Industria 4.0, o quarta rivoluzione industriale, si v. V. ZENO-ZENCOVICH, *Il concetto di “autonomia privata” ai tempi dei “Big Data”*, in D. Poletti, P. Passaglia (a cura di), *Nodi virtuali, legami informali: Internet alla ricerca di regole. A trent’anni dalla nascita di Internet e a venticinque anni dalla nascita del web*, Pisa, 2016, pp. 46-49. Per indicare, invece, l’auspicabile evoluzione di tale modello in un mercato basato sì, sul trattamento dei dati, ma rivolto anche a fini altruistici, da un punto di vista commerciale (e cioè, favorendo lo sviluppo delle piccole realtà imprenditoriali) e da quello pubblico, si è adoperata l’espressione “neomutualismo digitale”; sul punto si rinvia a P. VENTURI, F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, Milano, 2022; LEGACOOP-FONDAZIONE PICO (a cura

l'economia globale, in cui le "regole del gioco" sono stabilite dai giganti del c.d. GAAMM<sup>7</sup>, si è così affermata la c.d. "quinta libertà fondamentale": la libera circolazione dei dati<sup>8</sup>.

Il progresso tecnologico, per la sua estrema velocità, sfugge al controllo dello Stato. Nonostante le nuove tecniche digitali abbiano portato indubbiamente enormi vantaggi alla società, queste possono, in alcuni casi, minacciare i diritti fondamentali della persona e, in particolare, il diritto alla protezione dei dati personali<sup>9</sup>.

In Europa, la protezione delle persone fisiche con riguardo al trattamento dei dati è attualmente affidata al Regolamento europeo 2016/679 (*General Data Protection Regulation: d'ora in avanti, GDPR*)<sup>10</sup> che inten-

---

di), *Le cooperative e la sfida all'innovazione digitale: il neomutualismo in 10 tesi* ["Manifesto" sul neomutualismo digitale di Legacoop e Fondazione PICO], disponibile su: <https://pico.coop/risorse/il-manifesto/>.

<sup>7</sup> Google (Alphabet), Amazon, Apple, Meta Platforms (già Facebook) e Microsoft sono i colossi dell'*hi-tech* conosciuti come GAAMM (in precedenza, GAFAM) o *Big Five*. Il fatturato dei GAAMM, nel 2023, è stato di 378.972 miliardi di dollari. Per un'analisi del sistema dell'economia delle piattaforme digitali, si veda T. PASQUINO, A. RIZZO, M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020; A. QUARTA, *Mercati senza scambi. Le metamorfosi del contratto nel capitalismo della sorveglianza*, Napoli, 2020; A. SCHILLER, *Capitalismo digitale. Il mercato globale in rete*, Milano, 2000.

<sup>8</sup> F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*. I, *Dalla direttiva 95/46 al nuovo regolamento europeo*; II, *Il regolamento europeo 2016/679*, Torino, 2016, pp. 8-9. La "libera circolazione dei dati" è uno degli scopi che si propone il Regolamento UE n. 679/2016 (GDPR) e, prima ancora, la Direttiva 95/46/CE. La base giuridica dei due atti normativi, che costituiscono il cuore della disciplina per la protezione dei dati personali a livello europeo, corrisponde, infatti, all'art. 7 del TUE, sulla libera circolazione delle merci, delle persone, dei servizi e dei capitali nel mercato unico, per quanto riguarda la Direttiva (considerando 3, Dir. 95/46/CE); e all'art. 16, paragrafo 2, TFUE, per quanto riguarda il Regolamento (considerando 12, Reg. UE 2016/679). Quest'ultimo articolo del TFUE attribuisce agli organi dell'Unione il compito di assicurare la libera circolazione dei dati e al contempo garantire la protezione delle persone fisiche.

<sup>9</sup> La natura di diritto fondamentale del diritto alla protezione dei dati personali emerge dal Considerando 1 del Reg. UE 2016/679, dall'art. 16 del TFUE, ma, soprattutto, dalla Carta di Nizza, all'art. 8 (protezione dei dati di carattere personale), per cui: "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

<sup>10</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27

de allo stesso tempo assicurare la libertà di circolazione dei dati stessi<sup>11</sup>. La disciplina europea è, però, apparentemente ancorata a tecniche di tutela prettamente “individualistiche”. In particolare, un ruolo centrale viene attribuito al *consenso*<sup>12</sup>, i cui limiti sono stati evidenziati a più ri-

---

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. Sul Regolamento, si veda, tra i molti, R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), con la collaborazione di G. De Gregorio, *Codice della Privacy e Data Protection*, Milano, 2021; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; V. CUFFARO, G. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; P. VOIGT, A. VON DEM BUSSCHE, *The EU general data protection regulation (GDPR). A practical guide*, Cham, 2017; S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016.

<sup>11</sup> E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. e impr.*, 2018, pp. 107-109; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *NLCC*, 2017, p. 376. Lo scopo di bilanciare la protezione dei dati personali e la libera circolazione di tali dati è dichiarato fin dall'art. 1 del GDPR: “Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali”.

<sup>12</sup> *Ex art. 6 del GDPR il trattamento dei dati personali dei soggetti interessati è lecito se si fonda su una base giuridica, tra cui spicca il consenso dell'interessato al trattamento dei dati per specifiche finalità. All'art. 7 sono enumerate le caratteristiche che deve avere il consenso dell'interessato per essere ritenuto valido. Fin d'ora, sul consenso, ex multis, si veda V. BACHELET, *Il consenso oltre il consenso. Dati personali, contratto, mercato*, Pisa, 2023; C. IRTI, *Consenso “negoziato” e circolazione dei dati personali*, Torino, 2021; C. BASONATI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e imp.*, 2020, pp. 860-895; G. RESTA, V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, pp. 411-440; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 25 ss. Cfr. anche le *Linee guida 05/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, del Comitato europeo per la protezione dei dati, 4 maggio 2020, disponibili su: [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679\\_it](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_it) e le *Linee guida sul consenso ai sensi del Regolamento (UE) 2016/679* del Gruppo di lavoro Articolo 29, 6 luglio 2018, disponibili su: <https://ec.europa.eu/newsroom/article29/items/623051>; e le sentenze della CGUE, C-61/19, *Orange c. ANSPD*, 11 novembre 2020 e C-673-17, *Planet 49 GmbH c. Bundesverband der Verbraucherzentralen und Verbraucherverbände–Verbraucherzentrale Bundesverband eV*, 1 ottobre 2019.*

prese, e sul paradigma del diritto soggettivo sono costruiti i *diritti degli interessati* (artt. 12-22 GDPR)<sup>13</sup>.

Anche in ragione di ciò, i c.d. interessati, nel caso di violazioni dal carattere massivo delle loro libertà fondamentali, risultano spesso in una condizione di netto svantaggio nei confronti di chi tratta, a vario titolo, i loro dati<sup>14</sup>. Inoltre, a causa della strutturale asimmetria, economica e pratica, in cui si trovano, riscontrano forti difficoltà a far valere in giudizio i diritti loro attribuiti<sup>15</sup>. Il solo sistema dell'*enforcement* pubblico, basato sulle Autorità Indipendenti, non riesce, per mancanza di risorse, ad assicurare in via efficace il diritto alla protezione dei dati personali, né a garantire l'effettivo ristoro di eventuali danni subiti. Di conseguenza, le imprese continuano a perpetrare condotte illecite, che restano sostanzialmente impunte<sup>16</sup>. Tale situazione è imputabile principalmente a due caratteristiche della circolazione dei dati in rete: la sua portata *di massa e globale*.

Nella *data-driven economy*, l'aumento della capacità di elaborazione delle informazioni dei *computers* e degli altri dispositivi elettronici consente infatti di trattare un enorme quantità di dati, che vengono analizzati da preziosi strumenti: gli algoritmi intelligenti<sup>17</sup>. Negli ultimi anni,

---

<sup>13</sup> Lo sottolinea F. PIRAINO, *Il Regolamento*, cit., p. 379. Sui diritti dell'interessato, in generale, v. anche F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it.*, 2019, pp. 2789-2799; C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. Califano, C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, pp. 85-136.

<sup>14</sup> Le definizioni di "interessato" e di "titolare del trattamento" si trovano nello stesso Regolamento. All'art. 4, l'interessato viene definito come la persona fisica, identificata o identificabile, cui si riferiscono i dati personali (qualsiasi informazione); allo stesso articolo, il titolare del trattamento viene definito come: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".

<sup>15</sup> Si veda, a riguardo, quanto sottolineato nel report redatto dalla Agenzia europea per i diritti fondamentali (Fundamental Rights Agency, FRA), *GDPR in practice. Experiences of Data Protection Authorities*, 2024, disponibile su: <https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities> e nel report redatto dalla stessa agenzia già dieci anni prima, *Report: access to data protection remedies in EU Member States*, 2013, disponibile su: <https://fra.europa.eu/sq/publication/2014/access-data-protection-remedies-eu-member-states>.

<sup>16</sup> D. WRIGHT, *Enforcing Privacy*, in D. Wright, P. De Hert (a cura di), *Enforcing Privacy. Regulatory, Legal and Technological Approaches*, Berlino, 2016, p. 15.

<sup>17</sup> V. MAYER-SCHONBERGER, T. RAMGE, *Reinventare il capitalismo nell'era dei big data*, Milano, 2018, p. 7 ss.

sono state sviluppate tecniche di *big data analytics* sempre più evolute: vale a dire, strumenti di intelligenza artificiale<sup>18</sup>, soprattutto *software* di *machine learning*, in grado di ricavare informazioni e previsioni dai dati acquisiti. Il termine *machine learning*, apprendimento della macchina, sta proprio ad indicare la capacità di un sistema di intelligenza artificiale di imparare a svolgere un compito attraverso i dati recepiti, in alcuni casi senza essere programmato per farlo<sup>19</sup>.

---

<sup>18</sup> Il termine “Intelligenza Artificiale” fu utilizzato la prima volta nel 1955, quando dieci ricercatori proposero uno studio sulla possibilità di descrivere in modo analitico il funzionamento di “ogni aspetto dell’apprendimento o qualsiasi altra caratteristica dell’intelligenza” per consentire alle macchine di riprodurlo (F. COREA, C.G. FERRAUTO, F. FOSSA, A. LOREGGIA, S. QUINTARELLI, S. SAPIENZA, *Intelligenza artificiale. Cos’è davvero, come funziona, che effetti avrà*, Torino, 2020, spec. pp. 27-28). L’intelligenza artificiale fu definita da Raymond Kurzweil come l’arte di creare macchine che agiscono e pensano come esseri umani (“*The art of creating machines that perform functions that require intelligence when performed by people*”) o, comunque, in maniera razionale, parzialmente o totalmente in autonomia (R. RUSSEL, P. NORWIG, *Artificial Intelligence: A modern approach*, Hoboken, New Jersey, 2020, pp. 1-5; F. COREA, C.G. FERRAUTO, F. FOSSA, A. LOREGGIA, S. QUINTARELLI, S. SAPIENZA, *Intelligenza*, cit., p. 78). Ad oggi, a livello europeo, disponiamo di una definizione normativa del termine “intelligenza artificiale”, offerta dal Regolamento europeo 2024/1689, che stabilisce regole armonizzate sull’intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) n. 2018/858, (UE) n. 2018/1139 e (UE) n. 2019/2144 e le direttive 2014/90/UE, (UE) n. 2016/797 e (UE) n. 2020/1828 (Regolamento sull’intelligenza artificiale, Artificial Intelligence Act) che all’art. 3 definisce l’intelligenza artificiale: “un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall’input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali”.

<sup>19</sup> L’espressione “*machine learning*” fu coniata da Arthur Samuel, nello studio *Some studies in machine learning using the game of checkers*, in *IBM Journal of Research and Development*, 1959, pp. 210-229. I sistemi di *machine learning* si distinguono principalmente in *unsupervised*, *supervised* e *reinforced learning*. Mentre nei sistemi di *supervised machine learning* viene, sin da subito, assegnato un determinato risultato da produrre al *software* che, nel suo funzionamento, è comunque sempre controllato da un soggetto umano, nei sistemi di *unsupervised machine learning* manca tale controllo. Il *self learning* è, almeno in parte, un tipo di *unsupervised learning*. I *software* di *unsupervised learning* sono molto adoperati nel *marketing*, poiché sono in grado di individuare elementi comuni e categorie di dati (F. COREA, C.G. FERRAUTO, F. FOSSA, A. LOREGGIA, S. QUINTARELLI, S. SAPIENZA, *Intelligenza*, cit., spec. pp. 37-50). Una spiegazione riassuntiva dei diversi sistemi di *machine learning* è offerta dallo studio dell’EPRS (European Parliamentary Research Service), condotto a cura di G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence*, Study panel for the future of science and technology, Bruxelles, 2020, pp. 10-13.

I sistemi di *big data analytics* hanno bisogno di una grande quantità di informazioni per funzionare; attraverso la prassi migliorano la propria accuratezza, ma necessitano di un monitoraggio costante<sup>20</sup>. Possono sbagliare, ma il loro margine d'errore si riduce con l'utilizzo, e possono formulare *patterns*, predizioni e deduzioni, al di là degli *input* iniziali che gli sono stati forniti<sup>21</sup>.

I dati che i *software* di *machine learning* sfruttano sono *big data*, cioè: “*high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making*”<sup>22</sup>. Si tratta di una grande quantità di dati (*volume*), dotati di estrema varietà (*variety*), in termini di tempi di raccolta (*velocity*), tipologie e fonti<sup>23</sup>.

Alcuni dati vengono forniti spontaneamente dagli utenti. Altri sono dati c.d. “di scarto”, che rappresentano, in realtà, un rilevante plusvalore

---

<sup>20</sup> P. DOMINGOS, *L'algoritmo definitivo. La macchina che impara da sola e il futuro del nostro mondo*, Torino, 2016, pp. 1-21; pp. 261-266. Se non costantemente monitorati, gli algoritmi di *machine learning* scontano il problema dell'*overfitting*, e cioè si parametrano eccessivamente sui dati elaborati in sede di *training* generando, dunque, previsioni e risultati inattendibili rispetto ad altri tipi di dati, una volta messi in funzione.

<sup>21</sup> Alcuni *software* di *machine learning* (in particolare, quelli di *machine learning* non supervisionato che, nella maggior parte dei casi, funzionano con un sistema computazionale di reti neurali di elaborazione dei dati raccolti) identificano somiglianze e differenze tra individui e, partendo da tali “metadati”, svolgono analisi predittive (F. COREA, C.G. FERRAUTO, F. FOSSA, A. LOREGGIA, S. QUINTARELLI, S. SAPIENZA, *Intelligenza*, cit., p. 41 ss.). Vedi anche, sul punto, A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali*, cit., pp. 1186-1188. “Un passaggio nel processo complesso di rinvenimento nei dati di tendenze e modelli validi, nuovi, potenzialmente utili nonché comprensibili”, fondamentale nella formulazione di predizioni comportamentali, è il *data mining* (su cui U. FAYYAD, G. PIATETSKY-SHAPIRO, P. SMYTH, *From data mining to knowledge discovery: an overview*, in *AI magazine*, 1996, pp. 40-41 e T. ZARSKY, “*Mine your own business!*” *Making the case for the implications of the data mining of personal information in the forum of public opinion*, in *Yale Journ. of Law and Tech.*, 2003, spec. pp. 6-7; V. MAYER-SCHONBERGER, R. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, pp. 74-101).

<sup>22</sup> È questa la definizione di *big data* del *Gartner Information Technology Glossary*.

<sup>23</sup> A. MANTELERO, *La privacy*, cit., p. 1187. Più ampiamente, N. KHAN, M. AL-SAQER, H. SHAH, G. BADSHA, A.A. ABBASI, S. SALEHIAN, *The 10 Vs, Issues and Challenges of Big Data*, in *Proceedings of the 2018 International Conference on Big Data and Education*, 2018, pp. 52-56, disponibile su: <https://doi.org/10.1145/3206157.3206166>.

per le imprese ai fini di elaborare predizioni<sup>24</sup>. Ci si riferisce ai dati che emergono indirettamente dai comportamenti degli utenti nella rete, persino da eventuali errori di ortografia, dalla velocità con cui si effettua una ricerca, o dall'utilizzo di beni con elementi digitali. Si pensi al fenomeno dell'*Internet of Things*: tecnologie interconnesse che si scambiano informazioni acquisite da oggetti, orologi, macchinette del caffè e sistemi di sicurezza, e le trasmettono a fornitori di servizi e produttori<sup>25</sup>.

Gli scopi per cui gli strumenti di *big data analytics* possono essere impiegati sono vari, ma uno dei più ricorrenti è la profilazione, definita all'art. 4, n. 4, del Regolamento europeo n. 679/2016 come: "Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"<sup>26</sup>.

Mediante le tecniche di profilazione, il singolo viene classificato come componente di gruppi di soggetti con cui condivide alcuni tratti, che possono essere i più diversi; dall'orientamento politico o religioso, all'età, alla professione. La profilazione viene spesso utilizzata per prendere decisioni, di natura commerciale e non solo, che incidono sul comportamento e sulla vita delle persone; si va dalla pubblicità mirata, alla scelta se concedere o meno un mutuo, al calcolo dei premi assicurativi, alla selezione di candidati idonei per un posto di lavoro, alla sperimentazione di forme di c.d. giustizia predittiva, e molto altro ancora<sup>27</sup>. Essa può incidere perfino sulla libertà di autodeterminazione degli utenti in maniera profonda, per esempio orientandone le preferenze politiche<sup>28</sup>.

---

<sup>24</sup> Per tale ragione si è parlato di capitalismo estrattivo, dove chi produce i dati personali li cede a chi svolge attività d'impresa senza la percezione di star fornendo attributi di rilevante valore economico, consentendo alle imprese di produrre ricavi elevati a basso costo (F. PIRAINO, *Il Regolamento*, cit., p. 408).

<sup>25</sup> D.L. RUBINFELD, M. GAL, *Access barriers to Big Data*, in *Ariz. Law Rev.*, 2017, pp. 341-381. Con riferimento alla produzione costante di dati mediante le attività *online*, si rinvia a L. FLORIDI, *Il verde e il blu*, cit., p. 22, che descrive i consumatori come "producers".

<sup>26</sup> Considerando 63 e 71, art. 22 GDPR.

<sup>27</sup> B. MITTELSTADT, *From individual to group privacy in big data analytics*, in *Phil. & Tech*, 2017, p. 476. Si veda anche lo studio della Federal Trade Commission, *Big data, a tool for inclusion or exclusion?*, 2016, pp. 8-12.

<sup>28</sup> La profilazione è fondamentale anche ai fini di aumentare *l'engagement* nella c.d. *attention economy*; più gli utenti trascorrono il loro tempo *online*, più rilasciano

In estrema sintesi, il modello di *business* dei motori di ricerca e dei *social* è il seguente: i fornitori di prodotti commerciali pagano per ottenere uno “spazio” pubblicitario, o per collegare i loro prodotti alla formulazione di specifiche ricerche, e quindi ottenere un posizionamento favorevole. Si tratta di un mercato estremamente stratificato, in cui vi sono numerosi intermediari, ed in cui pochi attori svolgono una pluralità di funzioni<sup>29</sup>. L'attività di profilazione presuppone che i fornitori di servizi *online* dispongano di un'enorme quantità di dati personali, che vengono loro erogati, in un certo senso, come “corrispettivo” dei propri beni e servizi<sup>30</sup>. Si è innestata, dunque, una sorta di reazione a catena: più gli individui utilizzano i *servizi della società dell'informazione*, più producono dati, ed i prestatori di servizi migliorano, attraverso l'analisi di tali dati, i loro prodotti<sup>31</sup>. Di conseguenza, gli interessati dal trattamento dei dati sono, spesso, anche consumatori<sup>32</sup>.

---

dati nell'ambiente digitale, più le ipotesi predittive sono precise. Sul modello dell'*attention economy* e le sue implicazioni dal punto di vista giuridico, E. BIETTI, *The Data-Attention Imperative*, 2024, disponibile su: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4729500](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4729500).

<sup>29</sup> Si tratta generalmente di VLOP (*Very Large Online Platforms*) per utilizzare il termine adoperato dal Regolamento UE 2022/2065, relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE (regolamento sui servizi digitali, *Digital Services Act*), agli artt. 33 ss. Sul modello economico della *digital economy*, da un punto di vista di diritto della concorrenza, N. GUGGENBERGER, *Essential platforms*, in *Stan Tech. Law Rev.*, 2021, p. 237 ss.; J.M. NEWMAN, *Antitrust and zero price markets*, in *Wash. Univ. Law Rev.*, 2016, pp. 49-111, e R. POSNER, *Antitrust in the new economy*, in *Antitrust Law Journ.*, 2001, p. 925 ss. Specificamente sul modello Google, si rinvia a D. SRINIVASAN, *Why Google Dominates Advertising Markets*, in *Stan. Tech. Law Rev.*, 2020, p. 55 ss. e a E. BIETTI, *The Data-Attention*, cit., p. 20 ss.

<sup>30</sup> G. MALGIERI, B. CUSTERS, *Pricing privacy. The right to know the value of your personal data*, in *Comp. Law & Sec. Rev.*, 2018, p. 292 ss.

<sup>31</sup> La quantità di dati che gli utenti producono ogni giorno, è in costante aumento; si stima che la crescita sia del 30% ogni anno. Alla fine del 2025, probabilmente, si arriverà intorno agli 80 zettabytes (cfr. IDC, *Global DataSphere Forecast, 2021-2025: The World Keeps Creating More Data — Now, What Do We Do With It All?*, 2021).

<sup>32</sup> Sul rapporto tra diritto dei consumi e dei dati, si rinvia a S. PAGLIANTINI, *GDPR e consumerizzazione dei dati personali*, in *Giur. it.*, 2023, p. 2212 ss.; C. ANGIOLINI, *Una riflessione critica sulla complementarità fra norme sulla protezione dei dati personali e diritto dei consumatori nella disciplina dei profili patrimoniali del rapporto fra interessato e titolare del trattamento*, in C. Angiolini, D. Santarpia (a cura di), *La fattispecie “liquida”: quattro casi sintomatici*, Napoli, 2023, p. 7 ss.; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, e ai contributi del numero dedicato della rivista *Technology & Regulation*, C. BUSCH, C. GOANTA, K. KRYLA-CUDNA, M. LESZCZYNSKA, V. MAK, *Should data shape private law?*, in *Tech. Reg.*, 2022, p. 81 ss.

La “consumerizzazione del diritto dei dati” emerge in maniera particolarmente significativa dalla lettura della Direttiva UE 2019/770, sui contratti di fornitura di contenuti o servizi digitali e sulla vendita dei beni di consumo<sup>33</sup>. All’art. 3, infatti, la Direttiva riconosce la sussistenza, pur non classificandoli espressamente come contratti, di “casi” in cui la fornitura di un servizio digitale è condizionata alla fornitura, da parte del consumatore, dei propri dati<sup>34</sup>. Ancora, va ricordata l’estensione, da parte del legislatore europeo, delle tutele previste dalla Direttiva UE 2019/2161, per una migliore applicazione e una modernizzazione delle norme dell’Unione relative alla protezione dei consumatori (c.d. *Direttiva Omnibus*)<sup>35</sup>, ai contratti in cui il consumatore fornisce al professionista non il pagamento di un prezzo, ma i propri dati personali (art. 4, n. 2, lett. b)<sup>36</sup>. Da ultimo, il Regolamento UE 2022/868, *Data Governance Act* (DGA)<sup>37</sup>, ha definito la “condivisione” dei dati, al n. 10 dell’art. 2,

---

<sup>33</sup> Dir. UE 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, attuata in Italia agli artt. 130 *octies*-130 *vicies*ter del codice del consumo. *Ex multis*, in merito, G. VERSACI, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della Direttiva 2019/770/UE in una prospettiva comparata*, in *Riv. dir. priv.*, 2022, p. 207 ss.

<sup>34</sup> C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, pp. 505-506.

<sup>35</sup> Dir. UE 2019/2161 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell’Unione relative alla protezione dei consumatori. Anche l’art. 2 della Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) già definiva l’utente che adopera un servizio di comunicazione elettronica per finalità personali sia consumatore, sia interessato dal trattamento dei dati.

<sup>36</sup> Si leggano i Considerando 31-34 della Direttiva. La ricostruzione dei dati personali come attributi della personalità della cui dimensione patrimoniale si può disporre, pur essendo, ormai, quasi imposta dalla realtà empirica, non è certamente priva di criticità. Tuttavia, a nostro avviso, posto che il dato è senz’altro “parte” della persona in rete, come sostenuto da attenta dottrina, “ha poco senso sul piano concettuale chiedersi ‘cosa siano’ o come debbano essere qualificati i dati personali” (C. CAMARDI, *La dogmatica come “dispositivo immunitario” della scienza giuridica nel pensiero di A. Falzea. Come pensare la società digitale*, in *juscivile*, 2024, p. 22). Ciò che occorre è garantire la tutela della persona e della sua identità di fronte alle tecniche del capitalismo informazionale.

<sup>37</sup> Reg. UE 2022/868 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (*Data Governance Act*).