UNIVERSITÀ DI CATANIA
PUBBLICAZIONI DELLA FACOLTÀ DI GIURISPRUDENZA
Nuova serie
297

PERSONA E MERCATO NELLA SOCIETÀ DIGITALE

ATTI DELLE GIORNATE DI STUDI
(Catania, 13 dicembre 2022 e 4 maggio 2023)

a cura di
GAETANO GUZZARDI

Edizioni Scientifiche Italiane

UNIVERSITÀ DI CATANIA
PUBBLICAZIONI DELLA FACOLTÀ DI GIURISPRUDENZA
Nuova serie
297

PERSONA E MERCATO NELLA SOCIETÀ DIGITALE

ATTI DELLE GIORNATE DI STUDI
(Catania, 13 dicembre 2022 e 4 maggio 2023)

a cura di
Gaetano Guzzardi

Edizioni Scientifiche Italiane

Volume finanziato dal Dipartimento di Giurisprudenza dell'Università di Catania

L'inserimento di questo volume nella Collana "Università di Catania. Pubblicazioni della Facoltà di Giurisprudenza" è stato deliberato dal Consiglio del Dipartimento di Giurisprudenza a seguito di un parere favorevole dato da una commissione appositamente designata dallo stesso Consiglio.
Componenti della commissione valutatrice: Prof. Angelo Federico (Università di Messina), Prof. Giovanni Di Rosa (Università di Catania), Prof. Tommaso Mauceri (Università di Catania).

Guzzardi, Gaetano (*a cura di*)
Persona e mercato nella società digitale
Atti delle giornate di studi (Catania, 13 dicembre 2022 e 4 maggio 2023)
Collana: Pubblicazioni della Facoltà di Giurisprudenza dell'Università di Catania, 297
Napoli: Edizioni Scientifiche Italiane, 2024
pp. 172; 24 cm
ISBN 978-88-495-5568-4

80121 Napoli, via Chiatamone 7

Internet: www.edizioniesi.it
E-mail: info@edizioniesi.it

e-book ISBN 9788849555691

Indice

Nota del curatore 7

PARTE I

Strumenti giuridici e sviluppo tecnologico nel sistema agro-alimentare
Big Data e *blockchain* per la tracciabilità della filiera
Catania, 13 dicembre 2022

Alessandro Scuderi, *La* digital trasformation *nel sistema agro-alimentare* 11

Giuseppe Marino, *Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati* 19

Giuseppe Versaci, *La regolazione dei dati per l'agricoltura di precisione tra questioni generali ed esigenze settoriali* 59

Mariangela Ziccardi, *Digitalizzazione e innovazione tecnologica nei contratti di filiera agroalimentare* 75

PARTE II

L'identità personale nella società digitale
IoT & Human Enhancement Technologies
Catania, 4 maggio 2023

Gaetano Guzzardi, *Tutela della persona e sviluppo tecnologico nella società dell'informazione* 91

Emanuele Tuccari, *Note minime sull'asistematica disciplina del* neuromarketing 115

Mario Renna, *L'identità sicura: il banco di prova del* data breach 139

 ISBN 978-88-495-5568-4

Tommaso Mauceri, *Quale futuro per l'identità digitale. Rilievi conclusivi* 151

Gli Autori 155

ISBN 978-88-495-5568-4

NOTA DEL CURATORE

I contributi raccolti in questo volume costituiscono una rielaborazione – con l'aggiunta di minimi riferimenti bibliografici e giurisprudenziali e del necessario aggiornamento dovuto alla continua evoluzione tecnologica e normativa che caratterizza l'àmbito d'indagine – delle riflessioni svolte dagli Autori in occasione di due iniziative seminariali, rispettivamente, dal titolo "*Strumenti giuridici e sviluppo tecnologico nel sistema agro-alimentare.* Big Data *e* blockchain *per la tracciabilità della filiera*" e "*L'identità personale nella società digitale.* IoT *&* Human Enhancement Technologies", tenutesi a Catania il 13 dicembre 2022 e il 4 maggio 2023.

Il volume costituisce altresì un prodotto della ricerca condotta nell'àmbito del progetto "*I servizi di intermediazione nel mercato digitale. Profili ricostruttivi e questioni critiche*" (P.I. Gaetano Guzzardi), finanziato dall'Università degli Studi di Catania mediante il Piano di Incentivi per la Ricerca di Ateneo 2020/2022 – Linea di intervento 3 "*Starting Grant*".

Catania, 26.04.2024

Gaetano Guzzardi

ISBN 978-88-495-5568-4

PARTE I

Strumenti giuridici e sviluppo tecnologico nel sistema agro-alimentare

Big Data e *blockchain* per la tracciabilità della filiera

Catania, 13 dicembre 2022

Alessandro Scuderi

La *digital trasformation* nel sistema agroalimentare

Sommario: 1. Introduzione. – 2. La *"Digital trasformation"* nel sistema agroalimentare italiano. – 3. Conclusioni.

1. La trasformazione digitale è un processo che influenza qualunque aspetto della società umana. Si tratta di una trasformazione resa possibile e promossa dalle nuove tecnologie, che non si limita a potenziare i processi tradizionali d'innovazione e sviluppo ma che crea nuove forme d'innovazione caratterizzate da cambiamenti netti e rapidi e che riguarda ogni segmento della società, come l'economia, gli strumenti di comunicazione, il governo, l'informazione, l'arte, la medicina e la scienza. Non esiste un'unica definizione, specifica e riconosciuta, di un fenomeno così articolato e complesso. In questa indagine ci focalizzeremo sugli aspetti economici, per cui la "*Digital transformation"* sarà intesa come: il processo che ridisegna e rende più competitiva l'offerta complessiva del proprio business, tramite la trasformazione dei processi produttivi, l'analisi e l'ascolto delle esigenze di mercato per mezzo delle tecnologie digitali[1].

La definizione sottolinea l'importanza dell'aspetto innovativo della *Digital Trasformation*, affermando che la strategia da seguire non può essere solo quella di considerare un modello standard ma è necessario sviluppare tale trasformazione secondo le proprie caratteristiche aziendali, dato che la buona riuscita di una trasformazione digitale dipenderà anche e soprattutto dall'originalità di tale trasformazione.

Per comprendere il processo della "*Digital Transformation"* è necessario analizzare alcune tecnologie abilitanti, distinte in innovazioni sul prodotto-servizio e innovazioni sui processi, le quali assumono un significato strategico nel futuro dell'economia. In particolare, è utile descrivere i seguenti concetti chiave: *Disruptive Innovation*, *Internet of Things* e *Big Data*.

Il termine «*Disruptive Innovation*» è stato introdotto da Bower e Christensen[2] nel 1996, questi spiegano che le aziende che operano in mercati

[1] G. Vial, *Understanding digital transformation: A review and a research agenda*, in *Journal of Strategic Information Systems*, 2019, 28, pp. 118-144.

[2] J.L. Bower e C.M. Christensen, *Disruptive Technologies: Catching the Wave*, in *The Journal of Product Innovation Management*, 1996, 13, 1, pp. 75-76.

 ISBN 978-88-495-5568-4

maturi preferiscono focalizzarsi sulla «*sustaining innovation*», che potremmo tradurre come innovazione incrementale, contrapposta dagli autori alla «*Disruptive Innovation*». Nell'ottica di un investimento da pianificare, il rischio di puntare ripetutamente su un miglioramento graduale del prodotto di successo è decisamente minore rispetto a quello di progettare un prodotto o servizio *ex-novo*. Per questo motivo si procede all'aggiornamento dei prodotti introducendo funzionalità aggiuntive o migliorandone alcuni attributi così che il cliente possa percepire una variazione di valore.

Nell'ambito della digitalizzazione, «*Internet of Things*»[3] è un neologismo riferito all'estensione della rete internet al mondo degli oggetti e dei luoghi concreti: sempre più oggetti di uso quotidiano (ma non solo) sono dotati di un collegamento più o meno permanente alla rete internet nonché di sensori ed altri apparati in grado di monitorare e registrare le azioni e le abitudini delle persone. Il collegamento di detti oggetti (cosiddetti «dispositivi IoT») alla rete Internet permette lo scambio, l'archiviazione, la condivisione, e l'elaborazione di enormi flussi d'informazioni, in particolare di un numero elevato di dati personali.

Il termine «*Big Data*» nasce negli anni novanta del secolo scorso, ma la prima definizione riconosciuta, «un insieme di dati con dimensioni che vanno al di là della capacità di strumenti *software* comunemente usati per catturare, curare, gestire ed elaborare i dati», si ritrova all'inizio del 2000[4].

I dati disponibili si moltiplicano a un ritmo esponenziale, generati da sensori, da *social media*, da transazioni, da *smartphone* e da altre fonti. I «*Big Data*» possono rappresentare per le aziende di oggi un vero e proprio patrimonio, il cui potenziale può tuttavia esprimersi solo attraverso un loro impiego intelligente.

La trasformazione digitale procede a ritmi crescenti ma in maniera diversificata nei singoli Paesi. Per quanto riguarda l'Unione Europea, un quadro della situazione del fenomeno in esame si può desumere dal *Digital Economy and Society Index* (*DESI*)[5]. Il *DESI* è un indice composito che riassume gli indicatori rilevanti sulle prestazioni digitali dell'Europa e traccia i progressi degli Stati membri dell'UE sulla competitività digitale. L'indice DESI individua le seguenti dimensioni: connettività; capitale umano; integrazione della tecnologia digitale; servizi pubblici digitali.

Secondo la classificazione *DESI* i Paesi europei possono essere distinti in:

- *Lagging ahead*: sono i paesi che si "stanno attardando", questi hanno

[3] S.C. Mukhopadhyay e N.K. Suryadevara, *Internet of things: Challenges and opportunities*, Springer International Publishing, 2014.

[4] D. Laney, D. 3-D *Data Management: Controlling Data Volume, Velocity and Variety*, in *META Group Research Note*, February 6, 2001.

[5] European Commission. Digital Economy and Society Index 2022, consultabile all'indirizzo *https://digital-strategy.ec.europa.eu/en/policies/desi.*

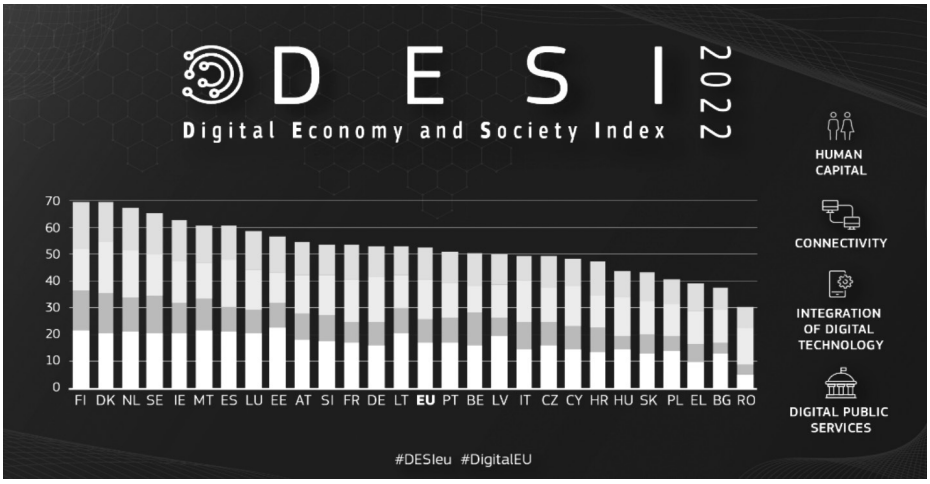
ISBN 978-88-495-5568-4

un punteggio superiore alla media UE ma nell'ultimo anno hanno rallentato la loro crescita registrando un incremento minore rispetto alla media Europea. In questo gruppo si trovano: Belgio, Danimarca, Finlandia, Irlanda, Lituania, Lussemburgo, Svezia e Regno Unito.

- *Catching up*: sono i paesi che "stanno rimontando", questi hanno un punteggio sotto la media UE ma nell'ultimo anno hanno registrato un incremento maggiore rispetto a quello medio europeo. Tra questi paesi, insieme a Spagna, Francia, Croazia, Lettonia, Romania e Slovenia, si colloca anche l'Italia.
- *Falling behind*: sono i paesi che stanno "restando indietro". Si collocano più bassi rispetto alla media EU28 sia per il valore del *DESI* che per l'incremento registrato. In questo gruppo si trovano Bulgaria, Cipro, Repubblica Ceca, Grecia, Ungheria, Polonia e Slovacchia.

Come riportato in figura l'Italia presenta un largo *gap* da recuperare, collocandosi al 18° posto nella classifica dei 28 Stati membri dell'UE. Ai primi posti si collocano i Paesi nordici quali Finlandia, Danimarca, Olanda e Svezia.

I dati relativi agli ultimi anni segnano per l'Italia un lento miglioramento ma è ancora evidente la distanza rispetto alla media europea, situazione allarmante se si tiene conto della crescente importanza dell'economia digitale, soprattutto nel futuro prossimo.



Digital Economy and Society Index in European Union States (2022 ranking)
Source: European Commission, 2023.

Nonostante siano stati fatti notevoli progressi in termini di ricorso alle tecnologie digitali da parte delle imprese, il dato più allarmante riguarda proprio lo stato della digitalizzazione delle aziende italiane: solo il 5,1% delle PMI utilizza l'*e-commerce*, a cui è imputabile appena il 4,8% del fat-

 ISBN 978-88-495-5568-4

turato complessivo delle imprese italiane. Nel rapporto di Unioncamere[6] viene anche evidenziato il differenziale rispetto al resto dell'UE in termini di esperienza di utilizzo degli utenti: ad esempio, solo il 35% acquista beni e servizi tramite internet, rispetto invece al 73% dei cittadini francesi e all'80% dei cittadini tedeschi. Dati preoccupanti, se si tiene conto dell'importanza che assumerà l'economia del digitale nei prossimi anni. Infatti, secondo uno studio realizzato dal *Boston Consulting Group*[7], per i Paesi del G-20 internet contribuirà a generare fino al 12,4% del PIL (come nel caso del Regno Unito), mentre in Italia l'economia di internet genererà il prossimo anno solo il 3,5% del PIL del Paese. Questo dato, comparato con la media di tutte le Nazioni del G-20 (5,3%) non è eccellente, ma è abbastanza per rendersi conto delle crescenti opportunità offerte dalle economie digitali, come testimonia l'incremento medio annuo dell'11,5% tra il 2010 e il 2022.

Le cause principali delle differenze con gli altri Paesi europei sono riconducibili essenzialmente alla mancanza di fiducia nelle tecnologie digitali e alla scarsa informazione dei cittadini circa gli effettivi vantaggi che ne derivano. Un problema che, come dimostrano gli stessi dati del *DESI*, non risparmia neanche il mondo delle imprese. In generale, internet non è visto come uno strumento così fondamentale per le aziende. In Italia il 40% degli imprenditori dichiara che internet non serve alla loro attività. Questo significa che su 10 imprenditori, almeno 4 non sono a conoscenza delle potenzialità che offrono la promozione dei propri prodotti sulla Rete e l'esistenza di un *touch point* digitale, oltre agli effetti positivi che l'*e- commerce* può avere sul fatturato aziendale.

2. La trasformazione digitale nel sistema agroalimentare gioca un ruolo cruciale per contrastare i fattori critici della globalizzazione e il crescente impatto dell'umanità sull'ambiente. In Italia, il potenziale di crescita del mercato delle soluzioni di «Agricoltura 4.0» e «*Farming* 4.0» è molto alto, ma ancora è ridotta l'adozione di tecnologie quali robot e sensori di *Precision farming.* Data l'importanza dell'*agrifood* per l'economia italiana, sono stati avviati progetti di formazione imprenditoriale "intelligente" in Agricoltura Digitale.

L'agricoltura digitale intende gestire la variabilità, che caratterizza l'agricoltura, in termini spaziali (da vasti territori alla singola fattoria) dei vari settori componenti, della singola unità produttiva. In termini temporali dalla preparazione del terreno, alla semina, alla raccolta. In questo contesto, le soluzioni di «Agricoltura 4.0» si integrano con quelle di «*Farming*

[6] *https://www.unioncamere.gov.it/spazio-europa-news-da-bruxelles/novita-legislative/digitalizzazione.*

[7] BCG *Releases* 2022 *Annual Sustainability Report* | BCG Report.

ISBN 978-88-495-5568-4

4.0», secondo un approccio basato su integrazioni di varie tecnologie ICT/geo-spaziali quali la geo-localizzazione dei veicoli per la guida assistita, il carotaggio/prelevamento di campioni, la raccolta dei dati sul campo, l'uso di macchine a dosaggio variabile, ecc.

Con il significativo progresso tecnologico degli ultimi decenni, l'Agricoltura 4.0 potrà trarre vantaggio da "contaminazioni" tra varie tecnologie, come ad esempio i due pilastri dell'industria geo-spaziale che riguardano i sistemi globali di navigazione satellitare (*Global Navigation Satellite Systems*, GNSS) e i sistemi informativi geografici (*Geographic Information Systems*, GIS). Tali sistemi possono essere combinati e integrati con sensori di prossimità (meteo, dendrometri, biosensori, ecc.), sistemi di connettività, protocolli e standard che garantiscano l'interoperabilità tra diversi dispositivi. Ciò rende possibile un monitoraggio remoto affidabile attraverso rilevamenti spazio-temporali e spettrali, in grado di monitorare i fenomeni a livello di singoli siti da varie posizioni altimetriche. Tali rilevamenti possono essere realizzate tramite i satelliti geostazionari (*Geostationary Earth Orbit*, GEO) e in orbita bassa (*Low Earth Orbit*, LEO), palloni sonda, droni/velivoli a pilotaggio remoto (*Remotely Piloted Aircraft/Unmanned Aerial Vehicles*, RPA/UAV), sensori di prossimità/identità *(Internet of Things,* IoT), ecc.

Ciò porta ad un'enorme quantità di dati rilevati/generati, aprendo la strada allo sviluppo di modelli di previsione e supporto alle decisioni (*Decision Support Systems*, DSS), reso possibile dalla disponibilità di servizi avanzati (GIS-*based*) di *(big) data management* "*as a service*", *Cloud, Big Data/Analytics*, Intelligenza Artificiale/*Machine Learning*, ecc. Tecnologie di *Augmented & Virtual Reality* (A&VR) sono poi in grado di rivoluzionare i sistemi di visualizzazione/*rendering* e DSS per *l'Agricoltura 4.0*, come ad esempio in applicazioni di manutenzione da remoto (AR) o simulatori di guida (VR), ovvero mescolando la realtà virtuale con tecnologie di scansione 3D (e.g. 3D *Building Information Modeling*-BIM) per progettare composizioni floreali disponibili in forma di ologrammi in cataloghi *online*.

Analogamente, la tecnologia blockchain applicata alla filiera agroalimentare consente di garantire un ambiente trasparente, sicuro e condiviso per la tracciabilità dei componenti e dei processi di trasformazione dei prodotti alimentari offerti al consumatore. Ad esempio, l'italiana *Foodchain* consente di raccogliere, registrare, analizzare, validare e certificare in modo sicuro (e decentralizzato) i dati, le informazioni e la documentazione in ogni fase della *supply chain*, attraverso le funzionalità aperte di *blockchain*, sostanzialmente, un *Enterprise Resource Planning* (ERP) integrato in *blockchain* attraverso l'uso del concetto di «smart contract».

A tale riguardo, le tecnologie geo-spaziali possono fornire una connessione tra mondo digitale e mondo reale, agendo da «agenti decentralizzati»

 ISBN 978-88-495-5568-4

(*trustless*) che abilitano gli «oracoli» (terminologia di Ethereum) richiesti per verificare/attivare le clausole degli *smart contract*. La *blockchain* può infatti essere integrata con gli oggetti fisici utilizzando piattaforme crittografiche incentrate sulla geo-localizzazione delle cose (*blockchain* + GIS / IoT), come fa *XYO Network*, una rete di localizzazione che rende il mondo fisico programmabile e accessibile agli sviluppatori (ad esempio di *smart contracts* Ethereum), facendoli interagire con il mondo reale come se fosse un'*Application Programming Interface* (API). I nodi della rete di localizzazione agiscono come «oracoli» per *smart contract* e robusti protocolli crittografati consentono di certificare la posizione dei componenti di sistema *Proof of Location* (PoL).

In generale, l'integrazione *blockchain*–IoT attraverso un sistema di localizzazione trasparente, sicuro e decentralizzato appare molto promettente, considerando che nel prossimo futuro le tecnologie «location-embedded» – ad esempio veicoli a guida autonoma, droni di consegna (UAV / RPA), comunità intelligenti che si sviluppano e autogestiscono autonomamente – renderanno la nostra vita dipendente dai dati di posizione e quindi la nostra sicurezza direttamente correlata all'accuratezza (e *cybersecurity*) dei dati di localizzazione utilizzati dai sistemi citati.

Combinando varie *feature* delle tecnologie *blockchain*, ad esempio quelle sviluppate da *Foodchain* e *XYO Network* eventualmente integrate con le moderne tecniche di *quantum computing*, si possono realizzare applicazioni per soddisfare la domanda sempre crescente dei consumatori a garanzia del territorio di origine dei prodotti agrifood. Infatti, oltre ai dati sull'ubicazione relativa (sensori di prossimità), si possono utilizzare specifici protocolli di archiviazione sulla *blockchain* (*Quadhash)* dei dati di posizioni *assolute* (*startup*LayerOne).

In sintesi, sono disponibili sistemi e tecnologie come GIS /infrastrutture geo-spaziali, reti *(ultra)broadband* (UBB) fisse e mobili, *Internet of Things* (IoT), Intelligenza Artificiale, *Blockchain,* Realtà Aumentata e Virtuale, ecc. Questi rendono possibile la fornitura di servizi digitali tramite piattaforme intelligenti per applicazioni di «*green & sustainable development*» (*Farming 4.0*, tracciamento della filiera alimentare, *e-health*, ecc.), utilizzando caso per caso le combinazioni più appropriate delle tecnologie citate. Con la disponibilità di competenze e tecnologie avanzate fruibili «*as a service*» nel *cloud*, e con il supporto di ricercatori ed esperti nei vari «*verticals*», è possibile realizzare iniziative (*market-driven*) per la fornitura di servizi «digitalizzati» a valore aggiunto nel campo dello sviluppo «*green*». Sarà necessario garantire agli utenti la *trasparenza* del processo cioè il mix di tecnologie avanzate impiegate per la generazione di valore nella *supply chain*.

Esiste un enorme potenziale di crescita e sviluppo di mercato nel settore agroalimentare. Solo il 2% della superficie agricola italiana utilizza robot e sensori di *Precision farming,* non uniformemente distribuita nelle varie

ISBN 978-88-495-5568-4

Regioni del Paese. L'agricoltura digitale (ICT-*assisted*) oscilla tra meno 1 e 4-5%, a fronte di 40-70% in Cina, Israele e USA. Il mercato dei sensori, e dei robot (senza contare quello, ben più ampio, dei servizi di *data science* collegati all'utilizzo/sfruttamento dei dati rilevati) è previsto pari a 4,5 miliardi di euro nel mondo (1 miliardo solo in Europa) entro il 2023, con una crescita media annuale (*compound annual growth rate,* CAGR) del 20%.

Ovviamente, il prerequisito per il successo della *Precision farming* è la formazione di adeguate competenze professionali a riguardo, in un settore caratterizzato da un livello di cultura aziendale e processi operativi basati più sul trasferimento di competenze e conoscenze generazionali che sull'innovazione e ottimizzazione dei processi produttivi.

Relativamente al settore dell'informazione geografica, la recente Norma UNI 11621-5:2018[8], definisce i relativi profili professionali, tenendo conto delle conoscenze, abilità e competenze richieste dalla continua trasformazione tecnologica, applicativa e organizzativa entro cui il professionista dell'informazione geografica si trova a dover operare. Essi devono essere in grado di fungere da divulgatori, acceleratori e gestori per l'utilizzo dei dati geo-spaziali all'interno di una *Spatial Data Infrastructure (SDI)* – ad esempio una comunità intelligente (agricola o meno). Ciò richiede nuovi profili professionali (di terza generazione), che secondo la nomenclatura dell'*European e-Competence Framework* (e-CF) possono essere messi in relazione con il quadro dei 23 profili professionali ICT di seconda generazione, onde coprire l'intero processo di business rappresentato dalla dimensione dell'e-CF, cioè dalle cinque aree di *e-competence* derivate dai processi business dell'ICT: pianificare (*plan*), realizzare (*build*), operare (*run*), abilitare (*enable*) e gestire (*manage*). Gli Stati Generali dell'Innovazione (SGI) e AMFM GIS Italia sono parte attiva di un'iniziativa dell'Agenzia di regolazione UNINFO (di cui SGI è Socio Onorario), sostenuta dall'Agenzia per l'Italia Digitale (AGID) per stabilire norme di regolamentazione dei profili di informazione geografica. Ciò ha portato all'introduzione di due profili specifici: *Geographic Information Manager* (GIM) e *Geographic Knowledge Enabler* (GKE). All'interno della rete di stakeholder, il GIM ha il compito di promuovere la crescita del livello di qualità e competenze tecniche, mentre il GKE deve principalmente promuovere la consapevolezza e il pensiero spaziale.

Oltre alle (pur rilevanti) competenze geo-spaziali, è però indispensabile che siano attivati percorsi formativi che preparino professionisti dell'agricoltura digitale, rendendoli capaci di interagire con le differenti competenze, tecnologie e processi trasversali di cui si è detto.

Il futuro del sistema agroalimentare dovrà affrontare questioni cruciali della "*Digital transformation*" nel settore *agrifood*:

[8] UNI 11621-5:2018. Attività professionali non regolamentate – Profili professionali per l'ICT – Parte 5: Profili professionali relativi all'informazione geografica. 26 aprile 2018.

 ISBN 978-88-495-5568-4

a) in che modo la trasformazione digitale stia impattando sulle filiere dell'agroalimentare;

b) lo stato attuale della digitalizzazione in agricoltura e nel comparto agroalimentare in genere;

c) come analizzare gli impatti della "*Digital transformation*" sulle filiere dell'agroalimentare (carne, pesce, settore caseario, ortofrutta) in modo da evidenziarne punti di contatto (cross-filiera) e implicazioni economiche e sociali;

d) quali tecnologie digitali hanno avuto e possano avere un maggiore impatto sulle singole filiere dell'agroalimentare, sui settori di contatto/intersezioni cross-filiera e sugli elementi trasversali alle diverse filiere;

e) quali sono le innovazioni digitali connesse all'evoluzione del comportamento del consumatore.

In relazione alle risposte che si avranno saranno definiti i possibili futuri scenari del sistema agroalimentare derivanti dall'implementazione della "*Digital trasformation*".

3. In questo scenario, la "*Digital transformation*" nel sistema agroalimentare si deve dividere fra un sistema ad alta intensità industriale e uno dove l'elemento chiave è la riscoperta di tecniche produttive naturali e rispettose dell'ambiente.

Tuttavia, considerando le esigenze ambientali, economiche e sociali, la "*Digital trasformation*" è fondamentale per migliorare la competitività del settore agroalimentare.

La remunerazione di tutte le fasi della filiera agroalimentare include corrette relazioni economiche e contrattuali tra tutti i soggetti: produttori agricoli, industria di trasformazione e distribuzione; maggior cooperazione e trasparenza, adozione di innovazioni di prodotto e di processo. Questa condizione è imprescindibile per consentire il miglioramento degli standard qualitativi, sociali e ambientali, anche nella logica del miglioramento dell'efficienza dei processi di produzione, d'innovazione e di *marketing*.

La *food economy* dovrebbe dunque costituire una risorsa in grado di rispondere alle esigenze più urgenti e immediate del pianeta, regolamentando la produzione di questa risorsa primaria, incentivando tecniche di produzione innovative e rispettose dell'ambiente ma soprattutto garantendo un'equa distribuzione delle risorse prodotte attraverso l'ausilio della "*Digital trasformation*".

ISBN 978-88-495-5568-4

Giuseppe Marino

Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati

Sommario: 1. Introduzione. – 2. La crisi della distinzione tra dati personali e non personali e la nuova nozione europea di dato. – 3. Gli strumenti di condivisione volontaria e cogente dei dati nei rapporti G2B e B2G tra *Data Governance Act* e *Data Act.* – 4. Il diritto di accesso e di condivisione dei dati degli utenti dell'*Internet of Things* nelle relazioni B2B e B2C nel regime del *Data Act.* – 5. *Segue*. Il rapporto tra il diritto di accesso e condivisione nel *Data Act* e il diritto alla portabilità nel GDPR. – 6. Obblighi di accesso e diritti di portabilità dei dati nel *Digital Markets Act.* – 7. Considerazioni conclusive.

1. Con l'entrata in vigore, l'11 gennaio 2024, del Reg. (UE) 2023/2854 denominato *Data Act* (di seguito indicato come DA)[1], l'Unione Europea chiude il cerchio di una complessa strategia di regolazione della "*data-economy*", formata da altri due recenti atti legislativi di notevole peso specifico come il *Data Governance Act* (DGA)[2] e il *Digital Markets Act* (DMA)[3], che ha messo in esponente il ruolo dei *big data*, dell'intelligenza artificiale e dell'*Internet of Things* (*infra* IoT)[4] e vede come traguardo la creazione di nuovi "Spazi europei comuni di dati" (*Common European Data Spaces*) distinti per area tematica[5].

[1] Regolamento (Ue) 2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

[2] Regolamento (Ue) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

[3] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

[4] A inaugurare l'azione del legislatore europeo era stata Comunicazione della Commissione Europea sul mercato unico digitale del 2015 intitolata Comunicazione della Commissione Europea (CE), Strategia per il mercato unico digitale in Europa (Bruxelles, 6.5.2015 COM(2015) 192 final), poi scandita dalla successiva dichiarazione programmatica intitolata Strategia europea per i dati del 2020 (Bruxelles, 19.2.2020 COM(2020) 66 final).

[5] Si veda da ultimo in tema il documento *Commission Staff Working Document on "Common European Data Spaces"* (Brussels, 24.1.2024 SWD(2024) 21 final). La prima proposta normativa relativa a uno Spazio europeo comuni di dati ha riguardato quelli sanitari: Proposta di Regolamento del Parlamento Europeo e del Consiglio sullo spazio europeo dei dati sanitari (3.5.2022 COM(2022) 197 final 2022/0140 (COD).

 ISBN 978-88-495-5568-4

Dall'angolo visuale della Commissione Europea, il problema strutturale che siffatta ondata regolatoria individua e prova a fronteggiare è rappresentato dall'insufficiente disponibilità di dati nel mercato e nella società europea tanto tra gli operatori economici che tra i soggetti pubblici, a causa del cospirare di un insieme di fattori qui solo sinteticamente richiamabili: la mancanza di chiarezza sui diritti dei soggetti, a vario titolo, coinvolti nella catena di produzione del valore dei dati; la diversa natura dei dati coinvolti (personali, non personali o misti); la varietà di fonti da cui essi derivano (*online*, *Internet of things*, *etc.*); la proteiforme declinazione delle rispettive funzioni[6]. In particolare, tali criticità si apprezzano sia con riguardo a informazioni aventi un immediato risvolto economico-mercantile di precipuo interesse per un riutilizzo innovativo da parte delle imprese, sia rispetto a dati che abbiamo, piuttosto, un primario rilievo sociale, per la loro impiegabilità in politiche di interesse pubblico e collettivo, come quelle di tutela della salute o dell'ambiente[7]. Il postulato concettuale di fondo su cui si articolano le menzionate politiche di massima propalazione dei dati nel tessuto economico europeo risiede in ciò, che la natura non rivale e *totipotente* dei dati implica che essi possano essere utilizzati reiteratamente per scopi completamente diversi da quelli per i quali erano stati in origine raccolti in un altro settore, al fine di favorire competizione e innovazione nelle dinamiche concorrenziali e progresso in quelle sociali[8]. In altri termini, se per le intrinseche proprietà economiche, il valore delle informazioni risiede nella capacità di essere impiegate in modo ripetuto e diverso senza disperdere utilità, la disciplina giuridica deve ora incentivare e promuovere, ora esigere e imporre, la diffusa circolazione dei dati in tutti gli ambiti delle relazioni economiche e sociali[9]. Già nella Comunicazione del 2017

[6] CE, Una strategia europea per i dati, cit., p. 7.

[7] Si vedano i contributi presenti nel volume Aa.Vv., *Rechte an Daten*, a cura di T. Pertot, Tübingen, 2020; nonché T. Tombal, *Business-to-government data sharing for environmental purposes*, in *Network Industries Quarterly*, 2022, pp. 7-8.

[8] Si leggano le considerazioni contenute nel *Commission Staff Working Document, Impact Assessment Report accompanying the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act) SWD(2022) 34 final*, p. 1. Già nella Strategia europea dei dati del 2020 (CE, Una strategia europea per i dati, cit., p. 8) veniva evidenziata l'importanza della disponibilità dei "dati per il bene pubblico", muniti cioè di una privilegiata destinazione al perseguimento di un interesse generale (si pensi ai dati sanitari e ambientali), e la necessità di migliorarne lo sfruttamento per "rendere disponibili più dati e migliorare il modo in cui i dati vengono utilizzati è essenziale per affrontare le sfide sociali, climatiche e ambientali, contribuendo a società più sane, più prospere e più sostenibili". Sulla rilevanza dei dati per l'interesse pubblico si veda l'articolata riflessione di J. Shkabatur, *The Global Commons of Data*, in *Stanford Technology Law Review*, 2019, p. 383 ss.; T. Ramge e V. Mayer Schönberger, *Fuori i dati! Rompere i monopoli delle informazioni per rilanciare il progresso*, Milano, 2021, p. 39.

[9] In dottrina si vedano I. Graef, *Market definition and market power in data: The case of online platforms*, in *World Competition*, 2015, pp. 473-505; Ead., *EU competition law,*

ISBN 978-88-495-5568-4

sull'economia europea dei dati, la Commissione Europea aveva sollevato la questione del limitato accesso ai dati generati dall'*Internet of Things* e "ai diritti d'uso dei dati co-generati (come i dati IoT in ambito industriale)" quale area prioritaria di intervento legislativo[10].

Su questi addentellati ha via via visto la luce un articolato apparato normativo, la cui prima epifania è rappresentata dal *General Data Protection Regulation* (di seguito menzionato come GDPR)[11] e dal diritto di cd. portabilità dei dati personali per le persone fisiche (art. 20); si annovera, altresì, il Regolamento sulla libera circolazione dei dati non personali del 2018, il quale promuove le pratiche di condivisione dei dati nelle relazioni *business to business* (B2B)[12]. Per ciò che riguarda le relazioni tra soggetti privati e pubblici va menzionata la *Open Data Directive*[13], che aspira a mettere i dati governativi a disposizione e al servizio degli attori privati. Ancora, a livello settoriale, sono state adottate legislazioni volte a governare l'accesso ai dati in possesso di imprese in un mercato puntualmente individuato, come ad esempio nel settore automobilistico[14], nella prestazione di servizi di pagamento[15], nei dati

data protection and online platforms: Data as essential facility, Alphen aan den Rijn, 2016, *passim*; H. Richter, *Europaisches Datenprivatrecht: Lehren aus der Kommissionsvorschlag für eine, Verordnung über europäische Daten-Governance"*, in *ZEuP*, 2021, p. 634.

[10] Cfr. Comunicazione della Commissione "Costruire un'economia dei dati europea" (Bruxelles, 10.1.2017 COM (2017) 9 final).

[11] Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE, [2016] GU L 119/1.

[12] Regolamento (UE) 2018/1807 su un quadro per la libera circolazione dei dati non personali nell'Unione Europea, [2018] GU L 303/59.

[13] Si tratta della Direttiva (UE) 2019/1024 del Parlamento Europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (cd. Open Data Directive). Il principio generale sancito dall'art. 3 è che "1. Fatto salvo il paragrafo 2 del presente articolo, gli Stati membri garantiscono che i documenti a cui si applica la presente Direttiva siano riutilizzabili per scopi commerciali o non commerciali, in conformità con l'articolo 1. 3: "1. Fatto salvo il paragrafo 2 del presente articolo, gli Stati membri assicurano che i documenti ai quali si applica la presente Direttiva in conformità all'articolo 1 siano riutilizzabili per scopi commerciali o non commerciali in conformità ai Capitoli III e IV. 2. Per i documenti di cui le biblioteche, comprese le biblioteche universitarie, i musei e gli archivi detengono i diritti di proprietà intellettuale e per i documenti detenuti dalle imprese pubbliche, gli Stati membri assicurano che, laddove sia consentito il riutilizzo di tali documenti, questi siano riutilizzabili per scopi commerciali o non commerciali, in conformità ai Capitoli III e IV".

[14] Regolamento (UE) 2018/858 relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE, [2017] GU L 151/1.

[15] Direttiva (UE) 2015/2366 sui servizi di pagamento nel mercato interno, [2015] GU L 337/35, in specie all'art. 67. In tema il contributo di G. Colangelo e A. Borgogno, Open Banking and the Ambiguous Competitive Effects of Data Portability, in Competition Policy International, in Antitrust Chronicle, 2021, p. 3 ss.

 ISBN 978-88-495-5568-4

concernenti la rete elettrica[16], nei sistemi di trasporto intelligenti[17], nelle energie rinnovabili[18] e nelle prestazioni energetiche degli edifici[19].

Rispetto a questi interventi ancora embrionali e frammentari, la triade legislativa formata da DGA, DMA e DA dà forma e sostanza a un *corpus* normativo composito ma organico, teso a promuovere e sostenere il libero flusso di informazioni attraverso la messa a partito di un nutrito *set* di regole di *condivisione* dei dati: espressione con la quale, stipulativamente, si possono intendere gli atti e le pratiche mediante i quali un soggetto che si trova nella disponibilità, anche solo materiale, dei dati ne fornisce l'accesso a destinatari diversi, direttamente o tramite un intermediario, ai fini dell'uso congiunto o individuale, alternativamente su base volontaria ovvero sulla scorta di previsioni cogenti. Il legislatore europeo impiega, invero, una ricca varietà di dispositivi tecnici volti a conseguire siffatto obiettivo della condivisione dei dati: nel corso dell'analisi si rinverranno ora obblighi di messa a disposizione per titolari dei dati (quali produttori di beni interconnessi o grandi piattaforme digitali), ora diritti di accesso a favore degli utenti, ora ancora diritti di portabilità e condivisione attribuiti al soggetto interessato o all'utente con riferimento sia a dati sia personali che non personale. Ci si trova, dunque, al cospetto di un'ampia gamma di iniziative, differenti in termini di portata e approccio normativo[20]: così alcuni interventi normativi sono di taglio generale, attraversando diagonalmente l'intero mercato unico, laddove altri sono pensati invece per uno specifico settore; alcuni impongono, in via cogente, la messa a disposizione dei dati, altri prevedono misure per facilitare la condivisione volontaria; taluni

[16] Direttiva (UE) 2019/944 relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la Direttiva 2012/27/UE, [2019] GU L 158/125; e Direttiva 2009/73/CE relativa a norme comuni per il mercato interno del gas naturale e che abroga la Direttiva 2003/55/CE, [2009] GU L 211/94.

[17] Direttiva 2010/40/UE sul quadro per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto Testo rilevante ai fini del SEE, [2010] GU L 207/1.

[18] Direttiva (Ue) 2023/2413 del Parlamento Europeo e del Consiglio del 18 ottobre 2023 che modifica la direttiva (UE) 2018/2001, il regolamento (UE) 2018/1999 e la direttiva n. 98/70/CE per quanto riguarda la promozione dell'energia da fonti rinnovabili e che abroga la direttiva (UE) 2015/652 del Consiglio.

[19] Proposta di Direttiva sul rendimento energetico degli edifici (rifusione), COM (2021) 802 definitivo, il cui testi definitivo è stato approvato dal Parlamento Europeo il 14 marzo 2024.

[20] Cfr. J. Drexl, *Designing competitive markets for industrial data - between propertisation and access*, in *JIPITEC*, 2017, p. 8 ss.; C. Ducuing, *Data as infrastructure? A study of data sharing legal regimes*, in *Competition and Regulation in Network Industries*, 2019, p. 21 ss.; I. Graef e J. Prüfer, *Mandated data sharing is a necessity in specific sectors*, in *Economisch Statistische Berichten*, 2018, pp. 298–301; T. Tombal, *Economic dependence and data access*, in *International Review of Intellectual Property and Competition Law*, 2020, pp. 70-98; Id., *Imposing data sharing among private actors - a tale of Evolving balances*, Alphen aan den Rijn, 2022.

ISBN 978-88-495-5568-4

introducono diritti generali di portabilità sui dati personali, altri attribuiscono diritti (asimmetrici) di accesso e condivisione di dati *tout court* nella disponibilità di altri soggetti[21]. L'elemento unificante va individuato, dunque, nella comune *ratio* pro-concorrenziale di cui queste previsioni sono latrici, miranti cioè alla promozione della concorrenza, della contendibilità e dell'innovazione nel mercato: obiettivi rispetto ai quali il paradigma della condivisione dei dati risulta, per le ragioni anzidette, funzionale[22].

Il presente contributo intende, pertanto, sottoporre ad analisi e mettere a sistema le singole previsioni nelle quali si possa rintracciare lo schema del cd. *data sharing*, distinguendo secondo la natura dei soggetti coinvolti nelle relazioni (B2G, B2B, *P2B, P2C*), soffermando l'attenzione sulle fattispecie di più immediata rilevanza civilistica. Sulla scorta di siffatta indagine, sarà possibile riflettere sulla configurabilità di un modello di dogmatizzazione della fattispecie che contempli una *moltiplicazione* e *coesistenza* di più situazioni soggettive sui medesimi dati, indifferentemente personali o non personali, intestate a titolari diversi facenti parte del processo di estrazione di valore economico dalle informazioni.

In ultima battuta, si svolgeranno alcune brevi considerazioni di ordine sistematico sull'odierna postura della disciplina europea dei dati, la cui evoluzione è contrassegnata da una marcata *bicefalia* tra la radice personalistica e lo sviluppo mercantilistisco-concorrenziale, che rischia di lacerare la tenuta del sistema: da un lato, specie nel diritto pretorile frutto dell'elaborazione della Corte di Giustizia dell'UE[23], continua a risaltare l'anima personalista

[21] Per una visione d'assieme si veda G. Colangelo, *European proposal for a data act. A first assessment*, in *Centre on Regulation in Europe (CERRE) Report*, 2022, p. 8; R. Feasey e A. De Streel, *Data sharing for digital markets contestability. Towards a governance framework, ivi*, 2020, p. 14 ss., entrambi disponibili su *https://cerre.eu/publications/*.

[22] Su questi aspetti in dottrina, tra gli altri, H. Richter, *The law and policy of government access to private sector data ('B2G data sharing')*, in *German Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare*, Baden-Baden, 2021, pp. 529-549.; J. Krämer, P. Senellart e A. de Streel, *Making data portability more effective in the digital economy*, in *CERRE Report*, 2020, *passim*, disponibile su *https://cerre.eu/publications; I. Graef e M. Husovec, Seven Things to Improve in the Data Act, 2022, disponibile su https://papers.ssrn.com/*; I. Graef, M. Husovec e J. van den Boom, *Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, in *Journal of European Consumer and Market Law*, 2020, p. 14; I. Graef, M. Husovec e N. Purtova, *Data portability and data control: lessons for an emerging concept in EU law*, in *German Law Journal*, 2020, pp. 1359-1398; P.G. Picht, *Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law*, in *Max Planck Institute for Innovation and Competition Research Paper 2022*, disponibile su *https://ssrn.com/abstract=4076842*.

[23] Nella recente elaborazione giurisprudenziale europea si vedano, in particolare, Corte giust. UE, 1° ottobre 2019, C-673/17, *Planet49*; Corte giust. UE, 11 novembre 2020, C-61/19, *Orange Romania*, Corte giust. UE, 4 luglio 2023, C-252/21, *Meta Platforms* (già

 ISBN 978-88-495-5568-4

nella quale alligna la tutela del diritto dell'individuo alla protezione dei dati personali, scolpito all'art. 8 della Carta dei diritti dell'UE, che vede ancora nel consenso informato dell'interessato il primario dispositivo di controllo degli attributi della persona[24]; dall'altro lato, nello *ius positum*, si alimenta

Facebook) c. *Bundeskartellamt*, reperibili integralmente in *www.curia.europa.eu*, ove anche disponibili anche le conclusioni dell'Avvocato generale Rantos, presentate il 20 settembre 2022. Sul caso Planet 49 e Orange Romania si vedano G. Marino, *Internet e tutela dei dati personali: il consenso ai cookie,* in *Jus civile*, 2020, spec. p. 410 ss.; A. Reinalter e S. Vale, *Cookie e consenso dell'utente*, in *Giur. it*., 2020, p. 79 ss.; S. El Sabi, *La Corte di Giustizia vieta le caselle di spunta preselezionate per il consenso all'uso dei cookie*, in *Giustiziacivile.com*, 2020; R. Cabazzi, *Utilizzo dei cookie e (nuova) tutela dell'utente interessato: la presa di posizione della Corte di Giustizia nel caso Planet49*, in *MediaLaws*, 2020, p. 316 ss.; C. Angiolini, *A proposito del caso Orange Romania deciso dalla Corte di giustizia dell'UE: il rapporto fra contratto e consenso al trattamento dei dati personali*, in *Nuove leggi civ. comm.*, 2021 p. 247 ss.; M.C. Meneghetti, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *MediaLaws*, 2021, p. 266 ss.; F. Esposito e L. De Almeida, *European Union Litigation, in European Review of Contract Law*, 2021, p. 87 ss.; G. Versaci, *Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità*, in *Nuove leggi civ. comm.*, 2023, p. 1131 ss. Per una nota di commento della decisione nel caso Meta Platform V. Bachelet, *La Corte di giustizia sul caso Meta: trattamento dei dati e "prezzo" del consenso*, in *Pactum*, 2023, p. 484 ss.; G. D'Ippolito, *Data Economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata*, in *Medialaws*, 2023; A.M. Hriscu, *Meta v Bundeskartellamt: The Lawfulness of Big Tech's Processing of Personal Data and the Relationship Between Data Protection and Competition Law*, in *EDPL*, 2023, p. 371 ss.

[24] Nell'ampio dibattito suscitato dal *General Data Protection Regulation* si veda, senza pretesa di completezza, V. Cuffaro, R. D'orazio e V. Ricciuto, *I dati personali nel diritto europeo*, cit.; Aa.Vv., *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di G. Finocchiaro, Bologna, 2019; Aa.Vv., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003* (Codice privacy), a cura di R. Panetta, Milano, 2019; Aa.Vv., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit.; Aa.Vv., *Persona e mercato dei dati: riflessioni sul GDPR*, cit.; Aa.Vv., *GDPR e Normativa Privacy. Commentario*, a cura di G.M. Riccio-G. Scorza-E. Belisario, Milano, 2018; V. Cuffaro, *Il diritto europeo alla protezione dei dati personali*, in *Contr. impr*., 2018, p. 1098 ss.; E. Lucchini-Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, *ivi*, p. 106 ss.; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr*., 2017, pp. 723-733; G. Finocchiaro, *Introduzione al Regolamento europeo sulla protezione dei dati, in Nuove leggi civ. comm.*, 2017, p. 1 ss.; A. Mantelero, *Responsabilità e rischio nel Reg. UE 2016/679, ivi*, p. 144 ss.; I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osserv. dir. civ. comm.*, 2018, p. 67 ss.; F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, p. 369 ss.; M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679, ivi*, p. 165 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo, ivi*, p. 410 ss.; M. Gomann, *The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement*, in *Common Market L. Rew.*, 2017, p. 567 ss.; P. Stanzione, *Il regolamento europeo sulla privacy: origini e am-*

ISBN 978-88-495-5568-4

la tensione concorrenziale del mercato europeo dei dati, all'espansione del quale è indefettibile un tessuto normativo di *favor* della circolazione delle informazioni tra gli agenti economici[25]. Sulla difficile convivenza e sui delicati equilibri tra rilievo individuale dell'autodeterminazione informativa del singolo e dimensione collettiva e relazionale dei dati, si gioca la partita odierna della regolazione europea della *data economy*[26].

bito di applicazione, in *Eur. dir. priv.,* 2016, p. 1249 ss.; S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità, ivi*, p. 513 ss.; Ead., *I requisiti del consenso al trattamento dei dati*, Santarcangelo di Romagna, 2016, *passim*.

[25] Per riflessioni monografiche sulla recente evoluzione della disciplina dei dati personali si vedano, senza pretesa di completezza, V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, Napoli, 2022, spec. p. 137 ss.; C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, spec. p. 50 ss.; R. Senigaglia, *Minore età e contratto*, Torino, 2020, p. 75 ss.; G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, spec. p. 105 ss., 149 ss.; C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, spec. p. 187 ss.; S. Thobani, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, spec. p. 160 ss.; A. De Franceschi, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, spec. p. 72 ss.

[26] La difficile convivenza tra l'impronta personalistica e quella mercantilistica emerge proprio dal GDPR: così sin dal considerando 2 si evince che «Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche». Si prende atto del fatto che «L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese» (considerando 5). Si mette poi in evidenza che «La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali» (considerando 6). In termini ancora più espliciti si afferma che «per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali» (considerando 7). Passando all'articolato normativo, l'intento del legislatore europeo di favorire la circolazione dei dati nel mercato interno affiora nell'incipit, ove l'art. 1, § 3, (invero riproduttivo dell'art. 1, § 2, dir. 95/46) è lapidario nello stabilire che «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». In letteratura, sottolineano la bicefalia della disciplina in commento M. Franzoni, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale*, in *Jus Civile*, 2021, p. 1 ss.; G. Alpa, *La "proprietà" dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., pp. 11 ss., 20 e 33; N. Zorzi Galgano, *Le due anime del GDPR e la tutela del diritto alla privacy*, in *Persona e mercato dei dati. Riflessioni*

 ISBN 978-88-495-5568-4

2. Il concetto di "dato personale" ha, sinora, rappresentato la pietra angolare attorno alla quale è stato eretto l'edificio normativo europeo in materia di dati. Coincidente con "qualsiasi informazione concernente una persona fisica identificata o identificabile" (art. 4, § 1, n. 1, GDPR), la nozione di dato personale si presenta come lata e dinamica e, com'è noto, è stata interpretata dalla giurisprudenza tanto europea quanto interna in termini che ne accentuano la flessibilità e l'ampiezza[27]. Sono quattro gli elementi che compongono l'architettura di questo concetto: l'informazione;

sul GDPR, cit., p. 35 ss. Apprezzano l'accentuazione della componente mercantilistica nella disciplina europea tra gli altri V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno,* in *Dir. inf*., 2018, p. 716 ss.; F. Bravo, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, in *Contr. impr.*, 2019, pp. 188-189. In posizione critica, invece, rispetto a questa scelta di politica del diritto, si colloca F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, cit., p. 375, secondo cui si nota «l'enfasi sul momento circolatorio dei dati personali rispetto alla sottolineatura delle implicazioni personalistiche del dato personale e alla conseguente istituzione delle premesse per giungere ad affermare una prevalenza assiologica delle seconda sulle ragioni sottese alla fruizione generale delle informazioni».

[27] Si pensi all'elaborazione della Corte di Giustizia UE nella sentenza sul caso *Patrick Breyer c. Bundesrepublik Deutschland*, causa C-582/14, del 19 ottobre 2016, commentata da A. Suman, *Indirizzi IP dinamici e Cybersicurezza: la conservazione dei "dati personali" degli utenti da parte dell'Internet provider nel caso Breyer*, in *Orientamenti della Corte di giustizia dell'Unione Europea in materia di responsabilità civile*, a cura di Alpa-Conte, Torino, 2018, p. 119 ss.: ove la Corte ha stabilito che «un indirizzo di protocollo Internet dinamico registrato da un fornitore di servizi di media online in occasione della consultazione, da parte di una persona, di un sito Internet che tale fornitore rende accessibile al pubblico costituisce, nei confronti di tale fornitore, un dato personale». In dottrina in tema v. F.Z. Borgesius, *The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition*, in *European data protection Law Review*, 2017, p. 130 ss. Un altro caso, deciso nel dicembre 2017, (CGUE, causa C-434/16, *Peter Nowak v Data Protection Commissioner*, 20.12.2017, di cui si può leggere un commento di K. Podstava, *Peter Nowak v Data Protection Commissioner: You Can Access Your Exam Script, Because It Is Personal Data*, in *European Data Protection Law Review*, 2018, p. 252 ss.) è particolarmente significativo per la definizione del concetto di "dati personali" in quanto fornisce un'interpretazione estensiva di cosa si debba intendere per "qualsiasi informazione riguardante una persona fisica". La CGUE ha ritenuto, infatti, che le risposte scritte fornite da un candidato a una prova di esame e le osservazioni dell'esaminatore in merito a tali risposte costituiscono "informazioni relative a quel candidato" e che sono, quindi, "dati personali". Da ultimo, ma solo in ordine di tempo, si segnala la decisione sul citato Caso *Planet49*, nella quale la Corte ha affermato che «l'installazione dei cookie […] rientra nel trattamento dei dati personali». Anche la giurisprudenza interna di legittimità accoglie un'accezione ampia della nozione di dato personale: Cass., ord., 7 luglio 2021, n. 19270, in *CED on line*, 2021; Cass., ord., 31 maggio 2021, n. 15161, *ivi*, 2021, secondo cui «il concetto di dati personali è idoneo a ricomprendere, stante l'ampiezza della nozione cui è approdata la Corte di Giustizia UE, qualsiasi tipo di affermazione su una persona e può includere quindi informazioni sia oggettive che soggettive, come valutazioni, concernenti la persona interessata, riguardando anche le dichiarazioni e le opinioni formulate tramite l'indirizzo di posta elettronica privata nel corso di uno scambio di corrispondenza elettronica».

ISBN 978-88-495-5568-4

la persona fisica; la riferibilità dell'informazione alla persona fisica; l'identificazione o, quantomeno, l'identificabilità di tale persona fisica. Con l'eccezione del riferimento alla nozione, dai contorni nitidi, di persona fisica, gli altri sintagmi sono caratterizzati da ampiezza e vaghezza semantica sì da contribuire ulteriormente a sfumare contenuti e limiti di questa categoria. Basti pensare all'anfibologia del concetto di "informazione" utilizzato tanto per far riferimento all'informazione come "contenuto", quanto al supporto materiale che immagazzina quel contenuto[28].

[28] In questa prospettiva, va menzionata la classificazione elaborata da Herbert Zech (H. Zech, *Information as a property*, in *JIPITEC*, 2015, p. 192 ss.; Id., *A legal framework for a data economy in the European Digital Single Market: rights to use data*, in *Journal of Intellectual Property Law & Practice*, 2016, p. 460 ss.; Id., *Data as a Tradeable Commodity*, in *European Contract Law and the Digital Single Market*, a cura di A. De Franceschi, Cambridge, 2016, p. 51 ss.), il quale propone di distinguere tra informazioni semantiche, ovverosia informazioni con un certo significato; informazioni sintattiche, rappresentate da una certa quantità di segni; e informazioni strutturali, ipostatizzate nella struttura di un oggetto fisico. Di «ambito semantico del termine informazione» che legittima «l'unificazione di informazioni (nel senso di notizie) […] e 'beni informazionali' (nel senso tanto di informazioni 'trattate' che di procedure tecniche del loro trattamento), che l'osservazione della realtà propone al giurista» già aveva parlato D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv*., 1998, pp. 339-340, il quale rinvia al classico scritto di P. Català, *Ebauche d'une théorie juridique de l'information*, in *Revue de droit prospectif*, p. 1 ss. Nella cornice di quel settore del sapere filosofico denominata "filosofia dell'informazione" si afferma che «*Data is a description of something that allows it to be recorded, analyzed, and reorganized*»: L. Floridi, *Philosophical Conceptions of Information*, in *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information*, a cura di Sommaruga, Berlino, 2009, p. 13 ss. In ordine all'interpretazione di tale definizione si veda il parere del gruppo Art. 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 20 giugno 2007 ('WP 136') (reperibile sul sito *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/ files/2007/wp129_en.pdf*). Nell'era della società algoritmica e della data economy il vero terreno di dibattito e di scontro intorno alla natura personale dei dati diviene quello dell'anonimizzazione e il confine con la regolamentazione dei dati non personali: in tema cfr. C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità,* cit., spec. p. 393 ss.; E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, p. 360 ss.; Ead., *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civ. comm.*, 2018, p. 1206 ss.; A. Nervi, *Il perimetro del Regolamento europeo: portata applicativa e definizioni*, in *I dati*, cit., p. 176; G. De Gregorio e R. Torino, *Privacy, protezione dei dati personali e big data*, in *La privacy digitale*, cit., p. 447 ss., spec. p. 472 ss.; G. D'acquisto e M. Naldi, *Big data e privacy by design. Anonimizpersonali nel diritto europeozazione, pseudonimizzazione, sicurezza*, Torino, 2017, p. 34 ss.; R. Ducato, *La crisi della definizione di dato personale nell'era del web 3.0, una lettura civilistica comparata*, in *Le definizioni nel diritto, Atti delle giornate di studio 30-31 ottobre 2015 Università di Trento*, a cura di Cortese-Tomasi, 2016, p. 143 ss. Nella letteratura straniera S. Wachter, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in *34 Computer*

 ISBN 978-88-495-5568-4

Nella letteratura giuseconomica, è diffusa una tassonomia dei dati personali, proposta da osservatori istituzionali come l'OECD[29] e il Gruppo Articolo 29[30], che opera una distinzione sulla base delle modalità di raccolta, la quale non illustra rilevanza esclusivamente teorica ma si rivela funzionale a definire portata e limiti dei diritti di portabilità e accesso disciplinati dal diritto dell'UE[31]. La prima categoria è rappresentata dai cd. *provided data*, ossia informazioni promananti dall'individuo interessato stesso. Essa fa riferimento all'informazione comunicata attivamente e consapevolmente dall'interessato (ad esempio, il nome, la data di nascita, la residenza, l'indirizzo di posta elettronica), la quale, nell'odierno assetto economico, esibisce invero un limitato rilievo commerciale, vista l'agevole reperibilità[32]. I dati possono anche essere forniti, ad esempio, ogni volta che un utente pubblica nuovi contenuti digitali (foto, video, post) sul proprio *account* di *social media*. Come si dirà meglio in seguito, il GDPR limita ai dati trasmessi dall'interessato alcuni diritti di controllo sui dati, come quello all'accesso (art. 15) e alla portabilità (art. 20).

Rilievo ben più significativo sul mercato digitale assumono sia gli *observed data* che i *generated data*, ovverosia i dati generati dalle interazioni tra un utente identificabile e il servizio digitale fruito o il dispositivo connesso impiegato[33]. I dati osservati e generati sono frutto di un'opera "creativa"

Law & Security Review, 2018, p. 436 ss.; P.M. Schwartz e D.J. Solove, *Reconciling Personal Information in the United States and European Union*, in 102 *California Law Review*, 2014, p. 877; B.J. Koops, *The Trouble with European Data Protection Law*, in 4 *International Data Privacy Law*, 2014, p. 4 ss.; E. Gratton, *If Personal Information Is Privacy's Gatekeeper, then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information*, in 24 *Alb. L.J. Sci. & Tech.*, 2013, p. 105; P. Ohm, Broken promises of privacy, in 57 UCLA Law Review, 2010, pp. 1701-1744.

[29] Si vedano gli articolati studi dell'Oecd, *Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, 21.3.2014; The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in *OECD Digital Economy Papers*, 176, 2011; *Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"*, *ivi*, 222, tutti reperibili sul sito *https://www.oecd.org/*.

[30] Cfr. *Article 29 Working Party, Opinion 4/2007 on the concept of personal data*, cit., p. 5 ss.

[31] Cfr. T. Tombal e I. Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?*, in *TILEC discussion paper*, 2022, pp. 3-5.

[32] All'interno della categoria, possono differenziarsi, a scopo puramente descrittivo, i dati divulgati da individui nel contesto di una richiesta di finanziamento ("*initiated data*"), dati creati quando si acquista un prodotto con una carta di credito ("*transactional data*") o dati condivisi (attivamente) tramite un social network online ("*posted data*"). Sebbene le persone interessate possano non essere consapevoli delle implicazioni della fornitura di questi dati, il fatto che questi dati vengano creati dovrebbe essere ovvio o almeno intuitivo.

[33] Gli esempi includono, tra l'altro, la cronologia delle ricerche degli interessati, la cronologia dei siti web visitati, i dati sul traffico e sulla posizione generati dall'uso di un'app o la frequenza cardiaca o il numero di passi raccolti da uno smartwatch. Cfr. *Article 29 Working Party, Opinion 4/2007 on the concept of personal data*, cit., p. 10.

ISBN 978-88-495-5568-4

comune tra utente e *provider*, poiché necessitano della compartecipazione e del contributo di entrambi i soggetti.

La terza categoria è costituita dai cd. *inferred data* ossia "dati desunti e dati derivati creati dal titolare del trattamento sulla base dei dati forniti dall'interessato"[34]. Si tratta della conoscenza derivante dalle informazioni personali, frutto di una costante e tecnologicamente raffinata opera di monitoraggio, analisi e sfruttamento delle attività svolte dall'utente *online* e per mezzo dei suoi *devices*. La capacità di una piattaforma digitale di generare inferenze perspicaci, innovative e accurate dai *dataset* accumulati può essere una decisiva fonte di differenziazione e di vantaggio competitivo nei mercati possono tradursi in servizi differenziati[35]. Si discorre, altresì, di "dati di seconda generazione", creati, dedotti o derivati da dati di prima generazione, forniti dall'interessato[36]. Essi esibiscono, pertanto, maggior qualità e valore aggiunto sul piano economico, in quanto *output* di un accurato processo tecnologico di analisi[37].

Infine, l'ultima categoria è quella dei cd. dati acquisiti (*acquired data*), ossia i dati ottenuti da terzi sulla base di un meccanismo volontario di condivisione (ad esempio, per mezzo dai *data broker*[38]) ovvero in attuazione di

[34] *Ibidem*, p. 10.

[35] Esempi ne sono la profilazione creata dal titolare del trattamento sulla base dell'analisi dei dati forniti dagli interessati, o i risultati di una valutazione della salute dell'interessato basata sui dati sanitari raccolti da un orologio intelligente.

[36] Cfr. R. Kemp, *Legal Aspects of Managing Data (White Paper)*, 2019, p. 8 disponibile su *http://www.kempitlaw.com/legal-aspects-of-managing-data/*.

[37] In questa prospettiva, la dottrina mette in luce come possa risultare miope l'esclusiva attenzione riservata in sede di tutela dei dati personali ai dati forniti volontariamente, materia grezza, input spesso di per sé scarsamente significativo, quando i rischi più significativi per i diritti fondamentali della persona discendono, principalmente, dall'output dalle inferenze e predizioni sui comportamenti, le preferenze, i gusti di una persona che gli operatori economici possono ritrarre, grazie alle tecnologie automatizzata dell'AI, a partire da un'ingente quantità di fonti di informazioni non convenzionali e non verificabili e sovente all'insaputa del soggetto cui si riferiscono. Sul punto v. S. Wachter e B. Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*, in *Columbia Business Law Review*, 2019, p. 13 ss.

[38] I "*data brokers*" sono ad oggi figure ancora misteriose quanto decisive nei meccanismi e nelle dinamiche di funzionamento del mercato dei dati personali e non personali. Essi sono rimasti quasi del tutto ignorati dagli studi giuridici europei e soprattutto dai legislatori a tutti i livelli. Pertanto, allo stato, si muovono in un campo pericolosamente sguarnito di un'adeguata regolazione giuridica, spesso nella penombra garantita dal fatto che non intrattengono un rapporto diretto con gli utenti, così sfuggendo alla disciplina consumeristica di matrice europea. La definizione di *data broker* è invero ancora incerta e dibattuta: possono essere definite come tali, le imprese che raccolgono informazioni personali e non personali e poi rivendono, condividono o comunque consentono l'uso di tali informazioni a vario titolo da parte di un altro operatore economico, a suo vantaggio o per il reciproco vantaggio. Esistono diversi tipi di *broker* di dati, la maggior parte dei quali non interagiscono direttamente con i consumatori, non essendo i soggetti che operano la raccolta di prima mano dei

 ISBN 978-88-495-5568-4

una regola cogente di messa a disposizione dei medesimi. Su questi aspetti si soffermerà l'attenzione nel corso del lavoro, ma può qui già ricordarsi

dati dai soggetti interessati: si tratta dei cd. *third party data broker*. Non sono figure nuove sul mercato: già dagli anni '60, i *broker* di dati raccoglievano informazioni, in particolare concernenti i clienti e consumatori offline. L'avvento di internet e le nuove possibilità tecnologiche hanno determinato un salto di qualità in siffatta attività, specie grazie all'utilizzo dei *cookie*. L'aspetto che preme indagare concerne l'utilizzo che dei dati, specie personali, fanno i *data broker*. La risposta è multiforme: vendono alcuni dei dati, anche grezzi, agli operatori economici interessati; impiegano le informazioni sugli acquisti compiuti dagli utenti per prevedere un interesse, analizzarne le caratteristiche; creano modelli predittivi da applicare ad altri consumatori dalle caratteristiche simili, attraverso una classificazione in cd. "*data segments*". Questi segmenti di dati vengono adoperati dagli inserzionisti che praticano il *targetized marketing*: alcuni apparentemente innocui (ad esempio, se un individuo acquista prodotti da cucina, può essere inserito in un segmento di dati chiamato "Interessato a prodotti da cucina" e ricevere pubblicità per prodotti da forno); altri ben più preoccupanti, come ad esempio informazioni sullo stato finanziario della persona, sul suo merito creditizio o assicurativo, sul tasso di utilizzo di una carta di credito etc. Il rischio evidente è la possibilità di una discriminazione delle persone legata a questi strumenti di circolazione dei dati, non governata da alcuna garanzia di sicurezza, accuratezza e controllo. Si pensi ancora alla delicatezza di un data segment che possa riguardare informazioni sensibili della persona, come quelle concernenti lo stato di salute e le conseguenti esigenze di farmaci o altri presidi sanitari. Guardando all'ambiente statunitense, i primi studi in materia hanno acclarato il ruolo centrale assunto dai broker nel mercato dei dati dei consumatori. Un report del *Committee On Commerce*, *Science And Transportation* ha rilevato che i broker di dati raccolgano informazioni sui consumatori da varie fonti, inclusi i social media e i rapporti contrattuali con le più svariate imprese. Si stima che Acxiom, uno dei più grandi data broker, disponga di circa ventitremila server che esaminano i dati di milioni di individui: *Us Senate Committee On Commerce, Science And Transportation (Staff Report), A Review of the Data Broker Industry: Collection, Use and Sale of Consumer Data for Marketing Purposes*, 2013). In questa direzione depone altresì il lavoro della *Federal Trade Commission, Data Brokers: A Call For Transparency And Accountability*, 2014, (reperibile su *http://www.ftc.gov/system/files/documents/reports/ data-brokers-call-transparency-accountability-report-federal-trade-commisitysion-may-2014/140527databrokerreport.pdf*). Negli USA, soltanto lo Stato del Vermont ha introdotto, nel maggio del 2018, una disciplina di protezione dei dati personali dei consumatori incentrata sulla regolamentazione delle attività dei broker di dati. Vi compare una prima definizione di data broker come «a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship». Un ampio studio della materia nella dottrina americana in B.A. Martin, *The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era*, in 105 *Iowa L. Rev.*, 2020, spec. p. 869, che sottolinea il problema dell'assenza di una regolazione compiuta a livello federale. Per ulteriori riferimenti cfr. altresì Y. Lev-Aretz e K.J. Strandburg, *Privacy Regulation and Innovation Policy*, in 22 *Yale J.L. & Tech,* 2020, p. 256 ss.; S.A. Elvy, *Paying for Privacy and the Personal Data Economy*, in 117 *Colum. L. Rev*., 2017, p. 1369 ss.; R. Lipman, *Online Privacy and the Invisible Market for Our Data*, in 120 *Penn St. L. Rev.*, 2016, pp. 777-787; T. Wu, *Blind Spot: The Attention Economy and the Law*, in *Antitrust Law Journal*, 2017, p. 25 ss.; F.A. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information*, Cambridge, 2015, p. 3 ss. Non manca in dottrina

ISBN 978-88-495-5568-4

come la seconda *Payment Services Directive* 2015/2366 (cd. PSD2) conceda ai prestatori di servizi di disposizione dei pagamenti e ai prestatori di servizi di informazione sui conti il diritto di acquisire le informazioni sui conti di pagamento degli utenti dei loro servizi (i consumatori), se questi ultimi vi abbiano acconsentito esplicitamente (artt. 64-67 PSD2)[39].

Rispetto a questa concezione *totalizzante* del dato personale, per una lunga fase evolutiva del diritto europeo, la nozione di dati *non* personali è stata pensata in termini puramente residuali quali "dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679" (art. 1, Reg. 2018/1807)[40]: essi possono essere, dunque, tanto i dati sia che non siano mai stati personali come quelli industriali generati dall'IoT (ad esempio raccolti dai sensori installati su macchine industriali)[41]; oppure i dati "anonimizzati" attraverso operazioni tecnologiche di tipo matematico, non qualificabili come dati personali dal momento che l'interessato non è più identificabile (considerando 26 del GDPR). A tal proposito, i dati anonimizzati non devono essere confusi con i dati "pseudonimizzati", che

chi sostiene che i veri attori protagonisti del brokeraggio di dati, ossia di pratiche diffuse e spregiudicate di vendita di dati personali degli utenti, siano soprattutto Facebook e Google: C.J. Hoofnagle, *Facebook and Google Are the New Data Brokers*, 2019, reperibile su *https://www.dli.tech.cornell.edu/blog/facebook-and-google-are-the-new-data-brokers*; A. Prat e T.M. Valletti, *Attention Oligopoly*, in *CEPR Discussion Paper*, 2018, pp. 1-40, secondo i quali, sul piano economico, i colossi del digitale siano i reali broker dell'attenzione sul mercato digitale. Spunti nella dottrina europea in Feasey e De Streel, *Data Sharing For Digital Markets Contestability Towards A Governance Framework*, cit., p. 35 ss.; R. Binns e E. Bietti, *Dissolving privacy, one merger at a time: Competition, data and third party tracking*, in *Computer law & Sec. Rev*., 2020, p. 3; P. Hacker, *Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive*, in *Data as counter-performance - Contract law 2.0?*, a cura di S. Lohsse, R. Schulze e D. Staudenmeyer, Baden Baden, 2020, p. 49 ss.

[39] In tema cfr., tra gli altri, G. Colangelo e O. Borgogno, *The data sharing paradox: BigTechs in finance*, in *European Competition Journal*, 2020, pp. 492-511.

[40] In dottrina si veda T. Tombal e I. Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?*, cit., p. 4; L. Somaini, *Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability*, in *EDPL*, pp. 88-90; Id., *The right to data portability and user control: ambitions and limitations, in MediaLaws - Riv. dir. Media*, 2018, p. 164 ss.; I. Graef *et al.*, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation,* in *European Law Review*, 2019, pp. 605-621; E. Egan, *Data Portability and Privacy: Charting a Way Forward, White Paper*, 2019, available at *https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf*; nonché T. Fia, *An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons*, in *Global Jurist*, 2021, p. 181 ss.

[41] Fra gli esempi specifici di dati non personali figurano gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei megadati, i dati sull'agricoltura di precisione che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua, o i dati sulle esigenze di manutenzione delle macchine industriali.

 ISBN 978-88-495-5568-4

rimangono soggetti alla disciplina di protezione dei dati personali a mente dell'art. 4, § 5, del GDPR, atteso che l'interessato può ancora essere re-identificato utilizzando informazioni aggiuntive[42].

Il modello normativo europeo di regolamentazione dei dati si è, dunque, tradizionalmente caratterizzato per una impostazione *monolitica*, per così dire "a tinta unica", imperniata sul costrutto concettuale *onnivoro* di dato personale, rispetto al quale tutto ciò che non ne viene fagocitato residua in chiave puramente negativa e oppositiva, quale dato *non* personale, privo cioè di una sostanza normativa propria. Questa scelta legislativa, dal rilievo non certo puramente lessicale, è stata foriera di un equilibrio normativo, sul quale per lungo tempo si è assiso il sistema europeo di governo dei dati, che ha visto in una posizione culturalmente e assiologicamente sovraordinata le regole sul trattamento dei dati personali e le correlate esigenze di protezione e controllo da garantire dell'identità e della riservatezza delle persone fisiche rispetto ad altre istanze potenzialmente emergenti in questa materia: quelle relative all'accesso e alla circolazione dei dati, al riutilizzo delle informazioni del settore pubblico e del settore privato, alla tutela della proprietà intellettuale (con le specifiche propaggini delle discipline sulla tutela delle banche di dati e dei segreti commerciali e aziendali)[43]. Nella tavola valoriale del sistema, ha senz'altro pesato la stretta correlazione del sistema di protezione dei dati personali con i diritti alla riservatezza e all'identità e la sua elezione nel *pantheon* dei diritti fondamentali della persona, limpidamente testimoniata dalla collocazione autonoma in una specifica disposizione della Carta di Nizza (art. 8)[44].

[42] Sul piano delle fonti istituzionali si veda CE, Communication on "*Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*" (Brussels, 29 May 2019, COM(2019) 250 final); Consiglio d'Europa, *Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* in *Council of Europe Treaty Series* n° 223; Article 29 Working Party, *Guidelines on the right to data portability*, 2016, p. 13 December 2016; Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 2014, *passim*.

[43] Per un'enfasi su questi aspetti gli studi dell'OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, in *OECD Publishing*, Paris, 2019; OECD, *Consumer Data Rights and Competition - Background note*, 2020, disponibili su *https://www.oecd.org/publications/*.

[44] I punti di riferimento nella ricostruzione di questo percorso rimangono quelli di S. Rodotà, *Tecnologie e diritti*, II ed., Bologna, 2021; Id., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997. Si vedano anche gli studi di Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., 1998, pp. 339-347; C. Camardi, *Mercato delle informazioni e privacy - riflessioni generali sulla L. n. 675/1996*, in *Eur. dir. priv.,* 1998, p. 1061 ss. Nella letteratura europea si vedano, *ex multis*, T. Streinz, *The Evolution of European Data Law*, in *The Evolution of EU Law*, a cura di P. Craig e G. de Búrca, III ed., Oxford 2021, pp. 902 ss., 915; P.C. Johannes, *Europäisches Datenrecht - ein Spickzettel*, in *ZD - Aktuell*, 2022, p. 1166 ss.

ISBN 978-88-495-5568-4

Negli ultimi anni, non sono, tuttavia, mancati i rilievi critici rispetto a questo assetto *unipolare* del sistema, rimarcando la tendenza della nozione di dato personale ad espandersi in modo incontrollato, specie nell'interpretazione della giurisprudenza europea, nonché la natura *per se* mutevole e oscillante del dato stesso[45]. Inoltre, si è evidenziata la circostanza per cui, nella maggior parte dei casi, le collezioni di *big data* siano di tipo "misto", cioè composte da dati sia personali che non personali[46]: come chiarito dalla Commissione, in tali casi il GDPR dovrà essere applicato alla totalità di un insieme di dati misti se essi siano "inestricabilmente collegati", pur se i dati personali ne rappresentino solo una modesta porzione (art. 2, § 2, Reg. 2018/1807)[47]. Sebbene il concetto di "inestricabilmente connesso" non sia puntualmente definito, dovrebbe essere inteso come comprendente situazioni in cui sarebbe impossibile, economicamente inefficiente o tecnicamente inapplicabile separare i dati personali da quelli non personali dell'insieme[48]. Tutti questi fattori aggravano il rischio, paventato dalla dottrina, che «in the near future everything will be or will contain personal data, leading to the application of data protection to everything»[49].

[45] Si vedano I. Graef *et al.*, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation*, cit., p. 605 ss.; I. Graef *et al.*, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal*, 2018, pp. 1359-1398; W. Kerber, *Governance of IoT Data: Why the EU Data Act will not fulfill its objectives*, in *SSRN Working Paper*, 2022, disponibile su *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436*; P. Picht, *Caught in the acts: framing mandatory data access transactions under the Data Act, further EU Digital Regulations Acts, and competition law, in Max Planck Institute for Innovation and Competition Research Paper* 22-05, 2022, disponibile su *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4076842.*

[46] Cfr. CE, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 2019, pp. 4 e 7.

[47] *Ibidem*, p. 9.

[48] *Ibidem*, p. 10. In dottrina cfr. I. Graef *et al.*, *Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation*, cit., pp. 610-611.

[49] Così N. Purtova, *The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law*, in *Law, Innovation and Technology*, 2018, p. 40 ss., che ritiene tale concetto destinato ad allargarsi a dismisura e a perdere perciò di ogni utilità euristica e, pertanto, propone di eliminare la qualificazione di personale o non personale. Così v. altresì I. Graef, R. Gellert e M. Husovec, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation*, in *TILEC Discussion Paper*, 2018, pp. 1-18, reperibile su *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189*. In questa direzione, che annulla la barriera esistente tra dati personali e non personali, vanno i *Principles for a Data Economy*, elaborati e approvati congiuntamente dall'*American Law Institute e dall'European Law Institute*, pubblicati nella loro versione definitiva il 27 settembre 2021, dopo quattro anni di lavori preparatori (consultabili sul sito *https://www.european- lawinstitute.eu/projects-publications/completed-projects-old/data-economy*) Agli antipodi non mancano

 ISBN 978-88-495-5568-4

Rispetto a questo assetto normativo, il nascente apparato regolatorio edificato dal legislatore europeo punta in direzione opposta: si assiste all'introduzione della nozione, autonoma e inedita, di dato *tout court* quale "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva" (art. 2, § 1, n. 1, DGA), che appare per la prima volta nel *Data Governance Act* e si ripete identica tanto nel *Digital Markets Act* (art. 2, § 1, n. 24) quanto nel *Data Act* (art. 2, § 1, n. 1)[50]. Siamo dinanzi ad un indicatore, elementare ma decisivo, dello spostamento del *baricentro* normativo della disciplina della *data economy*, che segnala un netto *revirement* rispetto alla pregressa impostazione imperniata sul caposaldo dei dati personali, per almeno due ordini di ragioni: anzitutto, perché delinea una categoria normativa e concettuale capace di abbracciare indifferentemente sia dati personali che non personali, volta ad attivare una disciplina tendenzialmente unitaria di apertura, condivisione e sfruttamento del dato; in secondo luogo, e ancor più significativamente, perché mette in esponente la dimensione "sintattica" e "strutturale" del dato, contenitore di stati del mondo, informazioni e conoscenze condensate in una rappresentazione digitale, più che quella "semantica" della sua riferibilità a un determinato individuo risaltata dai dati personali[51].

Ne discende la venuta alla luce di un nuovo statuto *olistico* ma *poliarchico* di regolazione del mercato dei dati, nel quale la primazia del principio di controllo e protezione dei dati personali si incrina e viene progressivamente affiancata, se non sopravanzata, da nuove esigenze di promozione dell'accesso, della disponibilità e della condivisione dei dati in funzione eminentemente concorrenziale[52]. In altri termini, si assiste, in chiave sistematica, alla

autori che criticano una lettura restrittiva del concetto di dato personale, esclusivamente puntato sull'input piuttosto che sull'output del processo di raccolta, analisi e profilazione: esso dovrebbe estendersi pertanto alle inferenze e predizioni elaborate, con mezzi puramente automatizzati, dai grandi operatori del web: così Wachter e Mittelstadt, *A right to reasonable inferences: re-thinking data protection law in the age of big data and AI*, cit., spec. p. 123, i quali propongono la creazione di un nuovo right to reasonable inferences «applicable to "high risk" inferences that cause damage to privacy or reputation, or have low verifiability in the sense of being predictive or opinion-based while being used for important decisions. This right would require ex-ante justification to be given by the data controller to establish whether an inference is reasonable. […] An *ex post* mechanism would allow data subjects to challenge unreasonable inferences, which can support challenges against automated decisions exercised under Article 22(3) of the GDPR».

[50] Cfr. G. Resta, *Towards a unified regime of data-rights?*, in *Governance of/through big data*, a cura di G. Resta e V. Zeno Zencovich, Roma, 2023, p. 643 ss.

[51] Sul punto le considerazioni di G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Governance of/through big data*, cit., pp. 607-608.

[52] Si veda l'impostazione metodologica di J. Drexl, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in *Digital Revolution: New*

ISBN 978-88-495-5568-4

prepotente emersione e al consolidamento di un *Datenwirtschaftsrecht* che si giustappone al tradizionale *Datenschutzrecht*[53]. Per questa via, battuta dalle più recenti iniziative legislative che si prenderanno in esame nel corso dello studio, si fa strada un approccio *promozionale* del legislatore europeo nella regolazione del mercato dei dati che – pur tenendo ferma, in via generale, l'applicazione della normativa di protezione dei dati personali – è formata da previsioni che si appuntano sui dati in quanto tali, privilegiando gli strumenti e le logiche dell'accesso e della condivisione rispetto a quelli del controllo e alla protezione.

3. Volgendo l'attenzione, anzitutto, alle relazioni tra soggetti pubblici e privati, l'odierna strategia normativa dell'UE espande il principio dell'*open data* dei dati nella disponibilità delle istituzioni pubbliche alle relazioni G2B e B2G, contemplando tanto congegni di condivisione volontaria quanto obblighi di messa a disposizione, parimenti destinati al riutilizzo di determinate categorie di informazioni protette in vista del raggiungimento di interessi collettivi[54].

In questo contesto, da un lato, il *Data Governance Act* inaugura un meccanismo di cd. *data altruism*, in virtù del quale gli attori pubblici possono condividere *volontariamente* i dati con quelli privati per molteplici finalità[55]. Dall'altro lato, gli artt. 14 e ss. del *Data Act* stabiliscono l'*obbligo* degli operatori privati di condivisione dei dati nella loro disponibilità a favore dei soggetti pubblici per "esigenze eccezionali"[56].

Challenges for Law, a cura di A. De Franceschi e R. Schulze, München-Baden-Baden, 2019, pp. 19, 21 ss.

[53] Così B. Steinrötter, *Das 'Datenwirtschaftsrecht' als neues Teilrechtsgebiet im Recht der Daten*, in *ZD*, 2021, 543; si veda in questo senso anche D. Staudenmayer, *Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz. Auf dem Weg zum Privatrecht der Datenwirtschaft*, in *EuZW*, 2022, p. 596.

[54] In dottrina vedi Colangelo, *European proposal for a data act. A first assessment*, cit., p. 5; nonché A. Vigorito, *Government Access to Privately Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models*, in *Eur. J. Comp. L. & Governance*, 2022, p. 515 ss.; H. Richter, *Zugang des Staates zu Daten der Privatwirtschaft*, in *ZRP*, 2020, p. 245; Id., *The Law and Policy of Government Access to Private Sector Data (B2G Data Sharing)*, in *Bundesministerium der Justiz und für Verbraucherschutz, Max-Planck-Institut für Innovation und Wettbewerb. Data Access, Consumer Interests and Public Welfare*, Baden-Baden 2021, p. 529 ss.; Y. Poullet, *From open data to reverse PSI - A new European policy facing GDPR*, in *Eur. Public Mosaic*, 2020.

[55] Nel definire l'ambito di applicazione del DGA, l'art. 3 prevede che "Il presente capo si applica ai dati detenuti da enti pubblici, che sono protetti per motivi di: a) riservatezza commerciale, compresi i segreti commerciali, professionali o d'impresa; b) riservatezza statistica; c) protezione dei diritti di proprietà intellettuale di terzi; o d) protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024".

[56] In tema cfr. H. Richter, *Access to private sector data for the common good,* in *CER-*

 ISBN 978-88-495-5568-4

Guardando al primo regime, gli articoli dal 16 al 25 del DGA prevedono misure tese a migliorare la condivisione *spontanea* dei "dati per il bene comune" a livello europeo[57]. Anzitutto, viene definita la "condivisione dei dati" come "la fornitura di dati da parte di un soggetto interessato o di un titolare di dati a un utente di dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio con licenze aperte o commerciali a pagamento o gratuitamente" (art. 2, n. 10, DGA). I nuovi soggetti della fattispecie di condivisione sono, su una sponda, il "titolare dei dati" e, sull'altra, l'"utente dei dati": il primo è soggetto pubblico che ha facoltà di concedere l'accesso e condividere i dati nella sua disponibilità; il secondo è soggetto, persona fisica o giuridica, al quale è attribuito il diritto di utilizzarli, tanto a fini commerciali che non commerciali[58].

Pur applicandosi in via generalizzata ai dati *sic et simpliciter*, permane una differenziazione di regime secondo la natura dei dati: se personali, il meccanismo di *data altruism*[59] viene definito come strumento volontario attraverso il quale gli interessati (persone fisiche, secondo la definizione fornita dall'art. 4, § 1, n. 1, GDPR) possono scegliere di condividere le

RE Report, 2023, pp. 5-7, disponibile su *www.cerre.eu*; Tombal, *Business-to-government data sharing for environmental purposes*, cit., p. 8; M. von Grafenstein, *Reconciling Conflicting Interests in Data through Data Governance: An Analytical Framework (and a Brief Discussion of the Data Governance Act Draft, the AI Regulation Draft, as well as the GDPR)*, in *HIIG Discussion Paper Series*, 2022, disponibile su *https://doi.org/10.5281/zenodo.6457735*.

[57] Su questi aspetti si soffermano A. Vigorito, *Government Access to Privately-Held Data: Business-to-Government Data Sharing. Voluntary and Mandatory Models*, in *Governance of/through big data*, cit., p. 697 ss.; G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., spec. p. 612 ss.

[58] Ai sensi dell'art. 2, n. 8, DGA, per "titolare dei dati" si intende una persona giuridica, compresi gli enti del settore pubblico e le organizzazioni internazionali, o una persona fisica che non è un soggetto interessato rispetto ai dati specifici in questione, che, in conformità al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso o di condividere determinati dati personali o non personali". Invece, l'"utente dei dati" è una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e ha il diritto, anche ai sensi del Regolamento (UE) 2016/679 nel caso dei dati personali, di utilizzare tali dati per scopi commerciali o non commerciali (art. 2, n. 9, DGA).

[59] All'art. 2, § 1, n. 16, il DGA definisce l'"altruismo dei dati" come "la condivisione volontaria dei dati sulla base del consenso degli interessati al trattamento dei dati personali che li riguardano, o i permessi dei titolari dei dati per consentire l'uso dei loro dati non personali senza chiedere o ricevere una ricompensa che vada oltre il risarcimento relativo ai costi che sostengono quando mettono a disposizione i loro dati per obiettivi di interesse generale come previsto dalla legge nazionale", ove applicabile, come l'assistenza sanitaria, la lotta al cambiamento climatico, il miglioramento della mobilità, la facilitazione dello sviluppo, della produzione e della diffusione di statistiche ufficiali, il miglioramento della fornitura di servizi pubblici, la definizione di politiche pubbliche o la ricerca scientifica nell'interesse generale".

ISBN 978-88-495-5568-4

informazioni che li riguardano[60]. In queste ipotesi, il DGA sancisce che la disciplina europea e nazionale in materia di protezione dei dati personali si applichi a qualsiasi dato personale trattato e che esso non valga a costituire una nuova base giuridica di liceità per il trattamento dei dati personali, rispetto a cui continuano a trovare applicazione le regole fissate dal GDPR (art. 1, § 3, DGA)[61]. Qualora invece si tratti di dati non personali, i titolari possono trasferire a utenti privati i dati nel loro controllo per scopi di interesse generale, commerciali o meno, finanche senza chiedere o ricevere un corrispettivo. Siffatte pratiche di condivisione altruistica dei dati si articoleranno, ordinariamente, su contratti di cd. *data-sharing*[62].

Nel disegno del legislatore europeo, un ruolo centrale nell'attuazione e diffusione capillare del *voluntary sharing* è affidato agli intermediari dei dati e ai servizi da essi prestati, ai quali è dedicato il Capo III del DGA[63], e

[60] Su questi profili si veda M. Shabani, *The Data Governance Act and the EU's move towards facilitating datasharing*, in *Molecular Systems Biology*, 2021, p. 2. In generale sull'idea della filantropia della conoscenza si vedano M. Taddeo, *Data Philanthropy and Individual Rights*, in *Minds and Machines*, 2017, pp. 1–5; R. Kirkpatrick, *A new type of philanthropy: donating data*, in *Harvard Business Review*, 2013.

[61] Nel loro parere congiunto sulla proposta di DGA (*EDPB-EDPS, Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, disponibile all'indirizzo *https://edps.europa.eu/dataprotection/ourwork/publications/edpsedpbjointopinions/edpsedpsjointopinionproposal_en*), il Comitato europeo per la protezione dei dati e il Garante europeo per la protezione dei dati hanno espresso le loro preoccupazioni sulla tensione esistente tra i principi di protezione dei dati di cui al GDPR e il modello di condivisione altruistica dei dati impostato dal DGA. Per quanto riguarda la terminologia, il parere congiunto ha rilevato la confusione e l'incompatibilità tra la nozione di "titolare dei dati" nel DGA e quella di "interessato" nel GDPR, nonché tra la nozione di "utente dei dati" nella proposta di DGA e quella di "responsabile del trattamento dei dati" nel GDPR: in entrambi i casi, potrebbero verificarsi conflitti tra i diritti e le prerogative derivanti da queste nozioni parzialmente sovrapposte. Il parere congiunto concludeva nel senso che la proposta di DGA "non tiene debitamente conto della necessità di assicurare e garantire il livello di protezione dei dati personali previsto dal diritto dell'UE", e pertanto "solleva serie preoccupazioni dal punto di vista dei diritti fondamentali" (p. 8 ss.)

[62] Cfr. Tombal, *Business-to-government data sharing for environmental purposes*, cit., p. 8. Per esempio, gli operatori telefonici che aumentano la loro condivisione B2G dei dati di localizzazione con un'autorità regionale possono consentire a quest'ultima di ottimizzare il suo sistema di trasporto pubblico, al fine di ridurre le emissioni di CO2 dei veicoli personali.

[63] Testimonia emblematicamente l'importanza attribuita dalla legislazione europea al ruolo degli intermediari dei dati il considerando 27 del DA: "si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti

 ISBN 978-88-495-5568-4

in particolare alle "cooperative di dati"[64], sulle quali si formulerà qualche considerazione in chiusura del lavoro. Lungo questa linea, la Commissione Europea ha, altresì, promosso la condivisione volontaria per scopi sociali, sviluppando una serie di "spazi di dati comuni europei", che dovrebbero portare alla disponibilità di ampi bacini di dati in domini di interesse pubblico come, in via esemplificativa, la protezione ambientale o quella della salute umana. Gli Spazi di dati europei rappresenteranno uno strumento chiave per sostenere e incentivare la creazione e lo sviluppo della logica dell'altruismo dei dati[65].

dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati. I servizi di intermediazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato, prevedendo nel contempo un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati. Ciò sarà particolarmente importante nel contesto della creazione di spazi comuni europei di dati, ossia quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile. I servizi di intermediazione dei dati potrebbero includere la condivisione bilaterale o multilaterale dei dati o la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, nonché l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati". Grande attenzione al ruolo dei *Data Intermediaries* e alla vasta gamma di contratti di scambio, cessione, condivisione di dati posti in essere in seno ai cd. data marketplaces è prestata dai menzionati *Ali-Eli Principles for a Data Economy*. Nel documento si legge che «*data marketplaces play an important role in the data economy*». In seno ai Principi, si qualifica come intermediario un soggetto che offre servizi di "*matchmaking*", che agisce al fine di facilitare le transazioni tra fornitori e destinatari dei dati. In quest'ambito, essi forniscono una serie di servizi accessori, come la fornitura dell'infrastruttura per trasferire i dati e l'eventuale pagamento, una classificazione reputazionale o la gestione dei re- clami per eventuali inadempimenti negli scambi. Quando i dati vengono forniti tramite un marketplace, per solito sono tre i rapporti contrattuali che si instaurano: il rapporto tra il fornitore di dati e l'acquirente, il rapporto tra il fornitore e il marketplace, e il rapporto tra il marketplace e l'acquirente. In dottrina cfr. H. Richter e P. Slowinski, *The Data Sharing Economy: On the emergence of New Intermediaries*, in *International Review of Intellectual Property and Competition Law*, 2019, pp. 4–29; F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contr. impr./Eur*., 2021, p. 199 ss.; A. Owusu, *Data sharing in the personal data economy. Does sharing mean caring?*, in *EJPLT*, 2023, p. 5.

[64] Per le prime riflessioni nella dottrina italiana v. F. Bravo, *Le cooperative di dati*, in *Contr. impr.,* 2023, p. 757 ss.; L. Petrone, *Il mercato digitale europeo e le cooperative di dati, ivi*, p. 800 ss.

[65] Cfr. CE, Documento di lavoro dei servizi della Commissione, Relazione sulla valutazione d'impatto che accompagna il documento "*Proposta di regolamento del Parlamento europeo e del Consiglio sulla governance europea dei dati: Un quadro abilitante per spazi comuni di dati europei (Data Governance Act)*", SWD (2020) 295 final, 25 novembre 2020 (Bruxelles), 22.

ISBN 978-88-495-5568-4

In pari tempo, la Commissione è consapevole del fatto che gli strumenti di condivisione volontaria non siano sufficienti ad attuare in modo compiuto la strategia di piena diffusione dei dati nell'economia europea. Per tale ragione, con il *Data Act*, impiegando un'opposta e complementare tecnica normativa, il legislatore europeo opta per previsioni imperative che impongono, a certe condizioni, la messa a disposizione di dati in possesso degli operatori economici privati a favore delle pubbliche amministrazioni[66]. Agli artt. 14 e ss. del DA, viene introdotto un vero e proprio obbligo di messa a disposizione dei dati in presenza di "esigenze eccezionali" del soggetto pubblico: si dispone, infatti, che "su richiesta, il titolare dei dati mette i dati a disposizione di un ente pubblico o di un'istituzione, agenzia o ente dell'Unione che dimostri la necessità eccezionale di utilizzare i dati richiesti" (art. 14, § 1). Preme sottolineare, tuttavia, che questo obbligo – come la restante disciplina in esame – non si applichi alle piccole e microimprese (art. 14, § 2).

Sul piano ermeneutico, il criterio chiave per determinare quando gli attori privati siano obbligati a condividere i dati con un ente pubblico è, quindi, l'esegesi della locuzione "esigenze eccezionali". Secondo il DA, quest'ultima sussiste in circostanze specifiche, come allorquando sia necessario rispondere, prevenire o assistere la ripresa da un'emergenza pubblica (art. 15, § 1, lett. b, DA). Per "emergenza pubblica" si intende una "situazione eccezionale che colpisce negativamente la popolazione dell'Unione, di uno Stato membro o di una parte di esso, con il rischio di ripercussioni gravi e durature sulle condizioni di vita o sulla stabilità economica, o il degrado sostanziale dei beni economici dell'Unione o dello Stato membro o degli Stati membri interessati" (art. 2, § 1, n. 10, DA). Peraltro, un'altra fattispecie tipizzata di necessità eccezionale può aversi allorquando la mancata disponibilità di dati impedisca a un ente del settore pubblico di svolgere un compito specifico nell'interesse pubblico e non è in grado di ottenere tali dati con mezzi alternativi tempestivi e convenienti (art. 15, § 1, lett. c, DA).

Alla luce di tale estensione e profondità della categoria delle esigenze eccezionali, ci si domanda se – prendendo a paradigma il grave e urgente problema del *climate change* – vi possa rientrare l'ipotesi della messa a disposizione di dati per obiettivi legati alla lotta al cambiamento climatico e al degrado ambientale. Da un canto, è possibile sostenere che le crisi climatiche siano emergenze pubbliche che è necessario affrontare o prevenire, in ossequio al disposto del menzionato art. 15, § 1, lett. a) e b) del DA. L'attuale condizione climatica potrebbe essere reputata una situazione eccezionale che rischia di avere ripercussioni gravi e durature sulle

[66] In tema si veda R. Podszun e C. Pfeifer, *Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission*, in *GRUR*, 2022, pp. 952, 958.

 ISBN 978-88-495-5568-4

condizioni di vita delle comunità o sulla stabilità economica. Pertanto, la condivisione di dati nelle relazioni B2G potrebbe essere imposta per affrontare (o prevenire) una specifica e imminente emergenza pubblica legata al clima o all'ambiente. D'altra parte, un simile obbligo non sussisterà allorché manchi il carattere eccezionale della situazione. Questa esegesi è, peraltro, corroborata dal considerando 58 del DA, che richiede circostanze "ragionevolmente prossime all'emergenza pubblica in questione", nonché dall'affermazione contenuta nel cd. *Impact Assessment* della Commissione Europea di accompagnamento al provvedimento normativo secondo cui "il criterio principale sarà il carattere eccezionale della situazione"[67].

In definitiva, l'introduzione gli obblighi di messa a disposizione dei dati, notevolmente invasivi della libertà d'impresa e dell'autonomia contrattuale degli operatori economici, devono esser limitati a scenari *sui generis* nei quali sia necessario affrontare emergenze pubbliche eccezionali: pertanto, il regolamento in parola potrebbe, al più, aspirare a integrare «existing reporting or compliance obligations in sectoral legislation that establish ongoing or recurring data exchange mechanism[s] between public institutions and the private sector»[68]. L'accesso "forzoso" della pubblica amministrazione a dati nella disponibilità dei privati non può che restare un'ipotesi liminale, relegata ad esigenze straordinarie di perseguimento dell'interesse pubblico[69].

4. Sul quadrante delle relazioni B2B e B2C, di maggior interesse per il civilista, e in particolare dell'utilizzo dei dati derivanti dall'*Internet of Things*, si concentra il *focus* del *Data Act*[70]. Rilevata l'insufficiente disponibilità e circolazione di dati in questo settore, l'obiettivo principale dell'interven-

[67] V. *Impact Assessment Report accompanying the Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, cit., p. 10.

[68] Così J. Drexl *et al.*, *Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, Munich, 2022, p. 52 disponibile su *https://www.ip.mpg.de/en/research/research-news/position-statement-on-the-eu-data- act.html*.

[69] Cfr. B. Martens, A. de Streel, I. Graef, T. Tombal e N. Duch-Brown, *Business to business data sharing: an economic and legal analysis*, in *EU Science Hub*, 2020, disponibile su *https://ssrn.com/abstract=3658100*; J. Krämer, D. Schnurr and S. Broughton Micova, *The role of data for digital markets contestability: case studies and data access remedies*, in *CERRE Report*, 2020, p. 4 ss. Feasey e De Streel, *Data Sharing For Digital Markets Contestability Towards A Governance Framework*, cit., p. 55 ss.; T. Tombal, *The rationale for compulsory B2B data sharing and its underlying balancing exercises,* in *Revue du Droit des Technologies de l'information*, 2022, p. 7 ss.

[70] Sull'impalcatura normativa del *Data Act* si vedano Aa.vv., *Data Act. An introduction,* Baden Baden, 2024, *passim*; J. Kramer, G. Colangelo, H. Kramer e D. Schnurr, *Data act: towards a balanced eu data regulation*, in *CERRE Report*, 2023, disponibile su *https//cerre.eu/publications*. Sulla proposta v. R. Podszun e P. Offergeld, *The EU Data Act and the Access to Secondary Markets*, in *Study for the Ludwig-Fröhler-Institut für Handwerkswissenschaften*, 2022, disponibile su *https://ssrn.com/abstract=4256882.*

ISBN 978-88-495-5568-4

to normativo è rappresentato dall'agevolazione dell'accesso e dell'impiego da parte dei consumatori e delle imprese, idonea, al contempo, a preservare gli incentivi a investire in modalità di generazione di valore economico e tecnologico *data-driven*. La Commissione rileva come, sebbene l'uso di prodotti interconnessi generi sempre più dati impiegabili come *input* dai servizi legati a questi prodotti, i consumatori e le imprese (soprattutto le *start-up* e le PMI) possano esercitare una limitata capacità di realizzare e mettere a frutto il valore dei dati generati poiché non in grado di vantare un controllo giuridicamente fondato su di essi. In questo contesto, infatti, i produttori sono sovente nella condizione di determinare, attraverso il controllo della progettazione tecnica del prodotto o dei servizi correlati (cd. *vendor lock-in*), quali dati vengono generati e come è possibile accedervi, sebbene la disciplina non attribuisca loro alcun diritto di esclusiva. Il legislatore europeo mette, altresì, in luce la coltre di incertezza giuridica che avvolge la possibilità che l'acquisto di un bene includa altresì un diritto di partecipazione al valore dei dati generati attraverso l'impiego del medesimo e dei servizi correlati. Ancora nebulosa risulta l'applicazione del diritto alla portabilità dei dati di cui all'art. 20 del GDPR ai dati generati dall'IoT: tale regolamentazione viene considerata insufficiente a incidere sui flussi di circolazione dei dati, dal momento che essa non trova applicazione ai dati non personali ed è limitato a quelli forniti dall'interessato su suo consenso ovvero oggetto di trattamento per la conclusione o l'esecuzione di un contratto, restando fuori dal cono applicativo i dati trattati sulla base di un altro fondamento di liceità previsto dall'art. 6 del GDPR. Analogamente, le legislazioni settoriali garantiscono soltanto che in alcuni peculiari ambiti (servizi di fornitura di energia elettrica, servizi di pagamento, settore automobilistico) i terzi possano avere accesso ai dati rilevanti[71].

Individuati questi "colli di bottiglia" nella piena diffusione dei dati promananti dai beni interconnessi nel mercato europeo, il DA parte dalla premessa che il produttore/progettista di un prodotto o di un servizio correlato vanta, il più delle volte, il controllo esclusivo *de facto* sui dati generati dagli utilizzatori dei beni interconnessi: tale fattore ostacola l'ingresso di operatori che offrono servizi post-vendita e servizi nuovi e, pertanto, la competizione sui cd. mercati secondari. Conseguentemente, il DA mette a punto un quadro normativo in seno al quale i beni interconnessi siano progettati e fabbricati e i servizi digitali prestati in modo tale che i dati generati dal loro utilizzo siano generalmente accessibili al loro utente[72].

[71] In proposito si veda il quadro emergente dai considerando dal 15 al 33 del *DA*, nonché le valutazioni espresse dalla Commissione *Impact Assessment Report*, cit., pp. 9-10, 15-16.

[72] In letteratura v. Colangelo, *European proposal for a data act. A first assessment*, cit., pp. 11-13; J. Kramer, *Improving the economic effectiveness of the b2b and b2c data sharing obligations in the proposed Data Act*, in *CERRE Report*, 2023, pp. 36-37.

 ISBN 978-88-495-5568-4

L'impianto normativo si fonda, in via primaria, sul costrutto del diritto all'accesso dell'utente – persona fisica o giuridica acquirente del bene o titolare di un diritto di godimento su di esso – sui dati generati dal prodotto interconnesso *by design*. L'art. 3 del DA impone l'obbligo ai *designer* e ai produttori al titolare dei dati di rendere accessibili tempestivamente e gratuitamente all'utente i dati generati dall'uso di IoT e/o servizi correlati, in modo diretto e per impostazione di *default*, ove tecnicamente possibile. Il "servizio correlato" viene definito, all'art. 2, § 1, n. 3, del DA, come un servizio digitale (inclusi anche i *software)* incorporato nel prodotto o ad esso interconnesso, essenziale per la sua *perfomance*: vale a dire che la sua assenza impedirebbe al prodotto di svolgere una delle funzioni o prestazioni sue proprie.

Sul punto, la disciplina europea squarcia, dunque, il velo di *anomia* che tradizionalmente ammanta l'ambito della produzione e che oggi viene invece investito da regole che incidono, in modo sempre più dirompente, sulle modalità e tecniche di progettazione di beni e servizi, in specie di carattere digitale e interconnesso.

Soltanto qualora l'accesso *by design and by default* non sia tecnicamente possibile, l'art. 4 del DA impone al titolare dei dati ("*data holder*") l'obbligo di mettere a disposizione dell'utente ("*user*") i dati generati dall'uso del prodotto o del servizio correlato. In questo contesto normativo, il "titolare dei dati" rappresenta il soggetto che ha, alternativamente, il diritto, l'obbligo o comunque la capacità – secondo il DA e, più in generale, il diritto dell'UE – di mettere a disposizione i dati generati dal IoT e garantirne accesso e circolazione (art. 2, § 1, n. 6, DA): si potrebbe, per ipotesi, trattare del *designer* quanto del produttore del bene interconnesso, così come del programmatore del *software* o del servizio digitale correlato da cui dipende il funzionamento del bene interconnesso.

In questa fattispecie, l'art. 4 del DA concede agli utenti il correlativo diritto di accesso ai dati – in prima persona o anche nella forma della condivisione con terzi (art. 5 del DA) – senza alcuna limitazione sul piano delle finalità di utilizzo, con l'eccezione del divieto di sviluppare prodotti in concorrenza con il prodotto da cui provengono i dati al fine di salvaguardare gli incentivi agli investimenti (art. 4, § 4, DA). Sul punto, si coglie l'estrema difficoltà di coordinare e rendere organica e coerente, sul piano assiologico, il coacervo di obiettivi generali di *policy* perseguita dal legislatore europeo, destinati fatalmente ad entrare in conflitto: qui la salvaguardia degli incentivi all'innovazione e la tutela dei segreti commerciali nei mercati primari prevale sul principio di libera circolazione dei dati e sulla promozione della concorrenza, che pure appaiono le linee direttrici dell'azione normativa europea in materia[73].

[73] Cfr. P.G. Picht, *Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law*, cit., p. 15 ss.

ISBN 978-88-495-5568-4

Inoltre, tali regole devono confrontarsi con le esigenze di tutela dei dati personali, in specie qualora l'utente cui sia riconosciuto diritto di accesso non sia l'interessato ai sensi dell'art. 4 del GDPR: sul punto, la norma stabilisce che – in modo invero alquanto generico – i dati personali dell'interessato possano essere messi a disposizione dell'utente sole ove sussista una delle basi di liceità di cui all'art. 6 del GDPR (art. 4, § 12, DA). Va notato che, sebbene il DA si allinei ai principi di minimizzazione del trattamento dei dati e di protezione dei dati *by design* scolpiti dal GDPR (considerando 8), le disposizioni che introducono il nuovo diritto di accesso e condivisione dei dati non prescrivono tuttavia né che i prodotti debbano essere progettati in modo da consentire ai soggetti interessati di utilizzarli in forma anonima (o nel modo meno invasivo possibile per la *privacy*) né che i titolari dei dati debbano anonimizzare i dati il più possibile[74]. Qualora si tratti, invece, di dati non personali, il titolare dei dati potrà utilizzare soltanto quelli autorizzati dall'utente sulla base di un accordo contrattuale di "*data sharing*", sul quale, per i limiti di questo lavoro, non è possibile soffermarsi (art. 4, § 13)[75].

Ove stabilisce che "su richiesta di un utente, o di una parte che agisce per conto di un utente, il titolare dei dati mette a disposizione di terzi i dati generati dall'uso di un prodotto o di un servizio correlato, senza indebito ritardo e a titolo gratuito per l'utente, con la stessa qualità di cui dispone il titolare dei dati e, ove applicabile, in modo continuo e in tempo reale", l'art. 5 DA sancisce il diritto di condivisione dell'utente dei dati con terzi ("*data recipients*") e, correlativamente, impone sui titolari dei dati l'obbligo di metterli a disposizione. Tale previsione si fonda sulla *ratio* secondo cui i dati co-generati da un utente e da un fornitore di un servizio o di un prodotto, attraverso l'uso di tale servizio o prodotto, devono essere liberamente disponibili per l'impiego da parte di tutti i soggetti che abbiano partecipato alla produzione di questo valore. Mentre l'accesso agli utenti deve essere concesso gratuitamente, il titolare dei dati può invece chiedere un compenso al terzo destinatario dei dati per condivisione da parte dell'utente quando a ciò sia tenuto a norma del DA (o di altra normativa del diritto dell'UE o nazionale attuativa della legislazione unionale)[76]. In tal caso,

[74] Al contrario, nel titolo dedicato alla condivisione dei dati tra imprese e amministrazioni pubbliche (B2G), il Regolamento sancisce che il titolare dei dati deve compiere sforzi ragionevoli per rendere anonimi i dati o, qualora tale anonimizzazione risulti impossibile, deve applicare mezzi tecnologici quali la pseudonimizzazione e l'aggregazione, prima di rendere i dati disponibili (si vedano gli artt. 17 e 18 DA). Sul punto in dottrina Colangelo, *European proposal for a data act. A first assessment*, cit., p. 16.

[75] Il *DA* dedica gli artt. 8-13 ai profili negoziali del contratto corrente tra data holder e user, nonché di quelli concernenti il data recipients. In letteratura v. J. Kramer, *Improving the economic effectiveness of the b2b and b2c data sharing obligations in the proposed Data Act*, cit., pp. 39-41.

[76] Preme notare che, oltre ai limiti descritti per quanto riguarda il tipo di dati, il tipo di

 ISBN 978-88-495-5568-4

il compenso deve essere ragionevole e le parti coinvolte (cioè il titolare e il destinatario dei dati) devono concordare condizioni eque, ragionevoli e non discriminatorie (art. 9 DA). Ciò rappresenta un notevole scostamento sia rispetto alla seconda direttiva sui servizi di pagamento (cd. PSD2) che al GDPR, dove l'accesso ai dati di pagamento e, in generale, la portabilità dei dati personali risultano del tutto gratuiti[77].

5. In chiave sistematica, i diritti di accesso e condivisione scolpiti dagli artt. 4 e 5 del DA instaurano un'ambivalente e ondivaga relazione con il diritto dell'interessato alla portabilità dei dati personali scolpito dall'art. 20 del GDPR e, più in generale, con il sistema di tutela dei dati personali, evidenziando profili di continuità, ma anche potenziali frizioni e cortocircuiti[78].

Il diritto alla portabilità dei dati personali, introdotto per la prima volta nel panorama normativo dall'art. 20 GDPR, rappresenta la punta d'avanguardia della tensione tra radice personalistica e propensione concorrenziale e circolatoria che attraversa la disciplina europea dei dati anche personali[79]. Esso si presenta come una situazione soggettiva complessa, formata

prodotti e il tipo di utilizzo da parte dei destinatari dei dati, la DA introduce ulteriori limiti all'ambito di applicazione del nuovo diritto di accesso e condivisione per quanto riguarda il tipo di titolari dei dati (esentando le PMI dagli obblighi di progettazione dei prodotti) e il tipo di destinatari dei dati (escludendo i gatekeeper dall'elenco dei potenziali beneficiari).

[77] Cfr. Colangelo, European proposal for a data act. A first assessment, cit., p. 16.

[78] Per un quadro di riferimento sui diritti dell'interessato, senza pretesa di esaustività, a partire dalla disciplina previgente cfr. A. Di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in *Trattamento dei dati e tutela della persona*, a cura di Cuffaro-Ricciuto-Zeno Zencovich, Milano, 1998, p. 225 ss.; G. Vettori, *Privacy e diritti dell'interessato*, in *Resp. civ. prev.*, 1998, p. 885 ss.; E. Bargelli, *sub art. 13 (Diritti dell'interessato)*, in *Tutela della privacy. Commentario alla legge 675/96*, a cura di Bianca-Busnelli, in *Nuove leggi civ. comm.*, 1999, p. 394 ss.; L. Mormile, *I diritti dell'interessato*, in *Libera circolazione e protezione dei dati personali*, II, a cura di R. Panetta, con prefazione di Rodotà, Milano, 2006, p. 1199 ss.; C. Lo Surdo, *Gli strumenti di tutela del soggetto «interessato» nella legge e nella sua concreta applicazione*, in *Diritto alla riservatezza e circolazione dei dati personali*, I, a cura di Pardolesi, I e II, Milano, 2003, p. 617 ss.; G. Salzano, *I diritti dell'interessato*, in *Il codice in materia di protezione dei dati personali. Commentario sistematico al D.Lgs. 30 giugno 2003 n. 196*, a cura di Monducci-Sartor, Padova, 2004, p. 19 ss. Sul GDPR si veda, in luogo di molti, F. Piraino, *I diritti dell'interessato nel Regolamento Generale per la protezione dei dati personali*, in *Giur. it*., 2019, p. 2777 ss.; A. Ricci, *I diritti dell'interessato*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 221 ss.; L. Di Lorenzo, *Spunti di riflessione su taluni «diritti dell'interessato»*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 237 ss.

[79] Nella dottrina italiana si veda M. Giorgianni, *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contr. impr*., 2019, p. 1387 ss. Sul diritto alla portabilità e sul suo ruolo di ponte tra la protezione dei dati personali e la promozione della concorrenza sul mercato digitale si vedano, senza pretesa di completezza, v. S. Troiano, Il diritto alla portabilità dei dati personali, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. Zorzi Galgano, Padova, 2019, p. 195; M. Borghi, *Portabilità dei dati e regola-*

ISBN 978-88-495-5568-4

dal diritto dell'interessato di «ricevere (…) i dati personali che lo riguardano forniti a un titolare di trattamento» (§ 1, prima parte), per un verso, e dal «diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti» (§ 1, seconda parte), nonché dal «diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile» (§ 2), per altro verso. L'ambito applicativo è soggetto a una duplice limitazione: anzitutto, per poter esercitare siffatto diritto, il trattamento dei dati personali deve essere fondato sul consenso dell'interessato ovvero essere necessario alla conclusione o all'esecuzione di un contratto corrente tra titolare del trattamento ed interessato, nonché deve essere svolto con mezzi automatizzati. In secondo luogo, come anticipato, il diritto di portabilità si riferisce esclusivamente ai dati "forniti" dall'interessato (*provided data*), non estendendosi, dunque, alle altre categorie dei dati generati, inferiti o acquisiti. Infine, il § 4 della previsione in parola dispone che l'esercizio del diritto alla portabilità non deve ledere i diritti e le libertà altrui[80].

Si è in presenza, pertanto, del riconoscimento all'interessato di un tipico potere di disposizione sui propri dati personali. La portabilità dei dati personali, quindi, va oltre la staticità peculiare del diritto di accesso, non

zione dei mercati digitali, in *Merc. conc. reg*., 2018, p. 223 ss.; G.C. Malgieri, *Il diritto alla portabilità dei dati personali*, in *Manuale per il trattamento dei dati personali*, a cura di Comandè-Malgieri, cit., p. 54; F. Pezza, *Diritto alla portabilità dei dati*, in *GDPR e normativa Privacy. Commentario*, a cura di Riccio-Scorza-Belisario, Milano, 2018, pp. 201 ss., 203; G.M. Riccio e F. Pezza, *Portabilità dei dati personali e interoperabilità, in I dati personali nel diritto europeo*, cit., p. 397 ss.; Ricci, *I diritti dell'interessato,* cit., pp. 179 ss. e 221-222; L. Bianchi, *Il diritto alla portabilità dei dati*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, a cura di R. Panetta, Milano, 2019, p. 223 ss.; E. Battelli e G. D'Ippolito, *Il diritto alla portabilità dei dati personali*, in *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 185 ss. Nel dibattito europeo cfr. L. Somaini, *Regulating the Dynamic Concept of Non-Personal Data in the EU: From Ownership to Portability*, in *EDPL*, 2020, pp. 84-93; I. Graef, T. Tombal e A. De Streel, *Limits and Enablers of Data Sharing An Analytical Framework for EU Competition, Data Protection and Consumer Law*, in *TILEC Discussion Paper*, 2019, pp. 1-35 e spec. p. 21, disponibile su *https://ssrn.com/abstract=3494212*; Aa.Vv., *The Right to data portability in the GDPR: Towards user-centric interoperability of digital services*, in *Computer Law & Security Rev*., 2018, p. 193 ss.; I. Graef, M. Husovec e N. Purtova, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal*, 2018, p. 1360 ss.; F. Weber, *Data portability and big data analytics. New competition policy challenges*, in *Conc. e merc.*, 2016, p. 59 ss.; B. Custers e H. Uršič, *Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection*, in *International Data Privacy Law*, 2016, p. 4; I. Graef, J. Verschakelen e P. Valcke, *Putting the Right to Data Portability into a Competition Law Perspective*, 2013, p. 63.

[80] Cfr. J. Krämer, P. Senellart, e A. de Streel, *Making Data Portability more Effective in the Digital Economy, in CERRE Report*, 2020, p. 18 ss.

 ISBN 978-88-495-5568-4

limitandosi alla possibilità di conoscenza dei dati oggetto di trattamento, bensì facilitandone la trasmissione e la circolazione nelle relazioni di mercato. Tale diritto esprime, manifestamente, una valenza eminentemente concorrenziale della disciplina dei dati personali, perseguendo l'obiettivo di incentivarne la diffusione e la riutilizzabilità da parte di più operatori sul mercato. In pari tempo, si preserva un nucleo di tutela dell'interessato, che può vantare una forma di controllo sulla circolazione delle proprie informazioni personali, attraverso l'esercizio del potere di accesso e trasmissione ad un diverso titolare. Come si legge nelle Linee guida sul diritto alla portabilità dei dati del Gruppo di Lavoro Articolo 29 per la protezione dei dati, la possibilità per l'interessato di trasmettere i propri dati a un diverso fornitore di servizi, appartenente anche a un altro settore di attività, «oltre ad ampliare il margine di controllo dei consumatori impedendo forme di "*lock-in*" tecnologico», promuove «l'innovazione e la condivisione di dati personali fra titolari del trattamento in piena sicurezza e sotto il controllo dell'interessato»: il fine principale del diritto alla portabilità si rinviene, quindi, nell'attribuzione all'interessato di un potere di controllo sulla circolazione dei dati, che ne facilita lo spostamento nel suo interesse e lo sottrae ai vincoli del *lock-in* tecnologico[81].

Guardando al rapporto con il *Data Act*, il nuovo diritto di accesso e condivisione dei dati esibisce aree di sovrapposizione e tratti differenziali, sia per eccesso che per difetto, rispetto al diritto di portabilità di cui all'art. 20 del GDPR. Per eccesso perché, in primo luogo, il diritto di accesso e condivisione dei dati di cui agli art. 4 e 5 ricomprende, sul piano oggettivo, tutti i dati, secondo la ricordata definizione, e non soltanto quelli personali; sul piano soggettivo, esso non è riservato unicamente all'interessato al trattamento dei dati personali, bensì riconosciuto all'utente, persona fisica ma anche giuridica, del prodotto interconnesso e/o del servizio correlato che quei dati genera; ancora, sul piano del *quomodo*, mentre l'art. 20 GDPR prefigura la portabilità dei dati come trasferimento *una tantum* ad un nuovo titolare, la condivisione concepita dall'art. 5 del DA è di tipo continuo e in tempo reale[82].

D'altro canto, l'impalcatura del DA si differenzia per difetto dal GDPR, atteso che quest'ultimo attrae nella sua orbita normativa, com'è noto, qualsiasi tipo di attività di trattamento di dati personali a prescindere dalla natu-

[81] Per l'importanza del ruolo del diritto alla portabilità nelle politiche europee sui dati personali si veda Art. 29 Data Protection Working Party, *Guidelines on the right to data portability*, cit., p. 6.

[82] In argomento v. Tombal e Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?,* cit., p. 7 ss.; J. Drexl *et al.*, *Position Statement of the Max Planck Institute for Innovation and Competition on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)*, cit., p. 15 ss.

ISBN 978-88-495-5568-4

ra delle relazioni di mercato o sociali nella quale si iscrive; viceversa, il DA si applica esclusivamente ai dati generati nell'utilizzo di oggetti interconnessi e dei servizi ad essi correlati, pur rappresentando quest'ultimo uno dei principali giacimenti di dati nel mercato. Sul piano soggettivo, da un lato, il DA esclude che gli obblighi di messa a disposizione dei dati incombano sulle micro o piccole imprese; dall'altro, ammette quali *data recipients* soltanto le imprese, le organizzazioni di ricerca e le organizzazioni senza scopo di lucro, escludendo i cd. *gatekeepers*[83] (la cui regolamentazione è dettata dal *Digital Markets Act*, al quale si volgerà l'attenzione nel prossimo paragrafo). Viceversa, il GDPR non contempla esclusioni o limitazioni sul piano soggettivo, né dal lato attivo né da quello passivo del rapporto di portabilità: qualunque titolare del trattamento è sottoposto a doveri e divieti previsti dal Regolamento; qualsiasi soggetto terzo può ricevere i dati personali dell'interessato ove questi eserciti il diritto di portabilità *ex* art. 20 GDPR. Infine, mentre il diritto alla portabilità del GDPR non implica alcun tipo di limitazione delle finalità d'impiego che i terzi possono fare dei dati portati (purché conforme alla normativa sulla protezione dei dati personali), il diritto di accesso e condivisione dei dati dell'IoT impedisce, come osservato, agli utenti e alle terze parti di sviluppare un prodotto che sia in concorrenza con il prodotto da cui provengono i dati[84].

Il DA potrebbe astrattamente contribuire, in via indiretta, a favorire e rendere maggiormente effettivo il diritto alla portabilità dei dati personali, qualora l'interessato sia anche l'utilizzatore del prodotto interconnesso e del servizio correlato[85]. L'art. 1 del DA prevede che "nella misura in cui gli utenti sono gli interessati", i diritti previsti da questa normativa integrino quelli di accesso e portabilità di cui al GDPR. Si pensi, in chiave esemplificativa, all'ipotesi in cui l'utente interessato chieda di condividere il suo profilo di consumo di elettricità ottenuto da un termostato intelligente con un servizio di confronto attiva lo scambio di dati tra il fornitore di elettricità e il fornitore del servizio di confronto[86].

[83] Sul punto v. I. Graef, T. Petročnik e T. Tombal, *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, in *Digital Society*, 2023, p. 13 ss.

[84] Cfr. J. Kramer, *Improving the economic effectiveness of the b2b and b2c data sharing obligations in the proposed Data Act*, cit., p. 38 ss.; A. Metzger e H. Schweitzer, *Shaping Markets: A Critical Evaluation of the Draft Data Act*, 2022, disponibile su *https://ssrn.com/abstract=4222376*).

[85] Sul punto l'art. 5, § 8, DA, dispone che "La mancanza di accordo, da parte del titolare dei dati e del terzo, sulle modalità per la trasmissione dei dati non ostacola, impedisce o interferisce con l'esercizio dei diritti dell'interessato a norma del regolamento (UE) 2016/679 e, in particolare, con il diritto alla portabilità dei dati di cui all'articolo 20 di tale regolamento"

[86] V. J. Kramer, *Improving the economic effectiveness of the b2b and b2c data sharing obligations in the proposed Data Act*, cit., p. 38.

 ISBN 978-88-495-5568-4

D'altra parte, il residuo potere di controllo che il GDPR assegna all'interessato per mezzo dell'esercizio della portabilità dei dati personali rischia di andar disperso nell'impianto normativo del DA, nella diversa ipotesi in cui utente e interessato non coincidano. Si apre, invero, un diaframma, già sul piano definitorio, tra la nozione di *user* formulata nel DA (art. 2, n. 12) – inclusiva, come detto, anche delle persone giuridiche – e quella di interessato dei cui dati personali si tratta (art. 4, n. 1, GDPR): si configura un potenziale scenario in seno al quale l'esercizio del diritto di condivisione da parte dell'utente imponga al *data holder* di fornire l'accesso e consentire lo sfruttamento da parte di terzi, anche in mancanza del consenso dell'interessato, persona fisica cui i dati sono riferiti[87]. L'art. 5, § 7, del DA dispone, invero, che "se l'utente non è l'interessato i cui dati personali sono richiesti, i dati personali generati dall'uso di un prodotto connesso o di un servizio correlato, sono messi a disposizione del terzo dal titolare dei dati solo se esiste una valida base giuridica per il trattamento a norma dell'articolo 6 del regolamento (UE) 2016/679": anche in mancanza del consenso dell'interessato, quindi, altre basi di liceità del trattamento possono giustificare una pratica di condivisione di dati personali di un interessato diverso dall'utente (art. 1, § 5)[88].

Vero è che, in termini generali, il DA fa salva la prevalenza della normativa di tutela dei dati personali e che, in particolare, l'art. 5, ult. par., dispone che la condivisione non deve ledere i diritti degli interessati ai dati personali. È evidente, tuttavia, che il pericolo celato da questa complessa interazione e sovrapposizione tra i diritti dell'interessato ai sensi del GDPR e i diritti e gli obblighi stabiliti dal DA, è di indebolire o conculcare le guarentigie previste per il diritto alla protezione dei dati personali degli interessati in seno agli accordi contrattuali di condivisione tra titolari e destinatari dei dati. Per di più, nessuna limitazione viene prevista per i dati sensibili, salvo un generico riferimento all'art. 9 del GDPR, esacerbando il rischio che la condivisione da parte dell'utente di informazioni estremamente delicate

[87] Sotto questo punto di vista, nel parere congiunto dell'EDPB-EDPS, *Joint Opinion 2/2022 on the Proposal of the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)*, 2022, disponibile su *https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22022-proposal-european_en*, il Garante europeo e il Comitato Europeo per la protezione dei dati personali hanno suggerito, in sede di commento alla proposta, di aggiungere alla definizione di utente quella di interessato e di differenziare chiaramente le situazioni in cui l'utente è anche interessato del trattamento (dunque quando i poteri ricadono sulla medesima persona fisica) dalla situazione in cui l'utente non coincide con l'interessato. Il testo definitivo del DA ha solo parzialmente accolto siffatti rilievi, rimanendo tuttavia la potenziale sovrapposizione dei poteri esercitati dall'interessato e utente.

[88] Al considerando 7 del DA si esclude espressamente, invece, che esso possa costituire autonomo fondamento di liceità del trattamento e della conseguente condivisione a mente dell'art. 6, § 1, lett. c), del GDPR.

ISBN 978-88-495-5568-4

riguardanti un diverso soggetto interessato possa determinare trattamenti discriminatori per quest'ultimo (si pensi alla trasmissione di dati relativi alla salute o biometrici o di quelli funzionali alla valutazione del *credit scoring* o dell'assicurabilità della persona)[89].

6. Se il DA si occupa di governare la circolazione dei dati generati dall'*Internet of Things*, il *Digital Markets Act* è destinato a disciplinare l'altro fondamentale serbatoio di dati per l'economia europea, ossia quelli generati nell'ambito dell'erogazione e fruizione dei servizi *online* attraverso le *big platforms* che dominano i mercati digitali.

In linea generale, il DMA mira a integrare, com'è noto, il diritto *antitrust* europeo con l'imposizione *ex ante* di un coacervo di obblighi di condotta in capo ai *gatekeeper.* Questi ultimi altro non sono che i grandi prestatori dei cd. servizi di piattaforma principale (tra gli altri, motori di ricerca, *social network*, inserzionisti pubblicitari, *browser web*, *cloud computing*, secondo l'elenco fissato dall'art. 2, § 1, n. 2, DMA), i quali soddisfino determinati criteri di rilevanza sul mercato europeo: capaci di esercitare un significato impatto sulla concorrenza, dislocati in una posizione, consolidata e duratura, di controllo dell'accesso a determinati settori commerciali (*gateaway*), sia attuale che potenziale (art. 3, § 1, DMA). Sul piano delle finalità generali, il DMA dichiara, sin dal suo *incipit*, di puntare all'armonizzazione delle norme destinate a garantire "mercati contendibili ed equi nel settore digitale in tutta l'Unione in cui sono presenti *gatekeeper*" (art. 1, § 1)[90].

La nozione di *gatekeeper* funge da perno attorno al quale si articola

[89] Per riflessioni su questi aspetti specie dalla prospettiva della intelligenza artificiale v. P. Femia, voce *Discriminazione (divieto di)*, in *Enc. dir., i Tematici, Contratto*, a cura di G. D'Amico, Milano, 2021, p. 499 ss.; G. Carapezza Figlia, *Decisioni algoritmiche tra diritto alla spiegazione e divieto di discriminare*, in *Persona e mercato*, 2023, p. 639 ss.; B. Parenzo, *Profilazione e discriminazione. Dal GDPR alla Proposta di Regolamento sull'IA*, in *Tecnologia e diritto*, 2023, p. 105 ss.; G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ*., 2021, 828 ss.; A.G. Grasso, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, 2023; R. Caterina, *Autonomia e intelligenza artificiale*, in *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, a cura di S. Giova e I. Prisco, Napoli, 2020, p. 142 ss.; G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir*., 2019, p. 211 ss.

[90] Per una visione generale del *Digital Markets Act* in dottrina cfr. C. Irti, *Piattaforme digitali, contratti e protezione dei dati personali*, in *I Contratti*, 2024, p. 5 ss.; G. Finocchiaro, *Responsabilità della piattaforma e tutela dei consumatori*, in *Giornale Dir. Amm*., 2023, p. 730 ss.; M. Colangelo, *La regolazione ex ante delle piattaforme digitali: analisi e spunti di riflessione sul Regolamento sui mercati digitali*, in *Nuove leggi civ. comm.*, 2023, p. 415 ss.; G. Guzzardi, *Il paradigma identitario nella società digitale*, in *Persona e mercato*, 2023, p. 526 ss.; M. Leistner, *The Commission's Digital Markets and Services Package - New Rules for Big Tech and Big Data*, in *GRUR Int*., 2021, p. 515 ss.

 ISBN 978-88-495-5568-4

una regolamentazione *asimmetrica*, che si pone in soluzione di continuità rispetto alla portata generale del GDPR e, seppur con alcune menzionate eccezioni, del *Data Act*. D'altro canto, assecondando lo stesso spirito del DA, il DMA impone ai *gatekeeper* obblighi di accesso e messa disposizione di dati *tout court*, personali e non, assicurando la portabilità dei medesimi, continua e in tempo reale, ai cd. "utenti finali" e "utenti commerciali": i primi sono identificati nelle persone, sia fisiche che giuridiche, che utilizzano i servizi di piattaforma di base offerti dal *gatekeeper*; e i secondi sono, piuttosto, imprese e professionisti che esercitano la loro attività economica attraverso la piattaforma di base, transitando necessariamente da punti di accesso al mercato degli utenti finali controllati dai *gatekeepers*[91].

Soffermando l'attenzione, tra i molteplici obblighi gravanti sui *gatekeepers*, su quelli concernenti la circolazione dei dati, è possibile operare, a livello descrittivo, una partizione in due categorie generali: alla prima vanno ascritti gli obblighi di concedere l'accesso ai dati a terzi ai fini della condivisione e della portabilità dei dati da parte di questi ultimi; alla seconda appartengono i doveri di condotta concernenti la raccolta, la combinazione e l'utilizzo dei dati da parte dei *gatekeepers*[92].

Volgendo l'attenzione al primo gruppo di regole, con riferimento agli utenti finali, ai sensi dell'art. 6, § 9, DMA, "il gatekeeper fornisce, su richiesta e a titolo gratuito, agli utenti finali e a terzi autorizzati da un utente finale l'effettiva portabilità dei dati forniti dall'utente finale o generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base, anche fornendo a titolo gratuito strumenti per agevolare l'effettivo esercizio di tale portabilità dei dati, nonché fornendo un accesso continuo e in tempo reale a tali dati". Come chiarito anche dal considerando 59, la previsione si fonda sul presupposto per il quale i *gatekeepers* hanno accesso a moli sterminate di dati, raccolti nell'ambito della prestazione dei servizi di piattaforma di base, nonché di altri connessi servizi digitali. Al fine di evitare limitazioni del livello di concorrenza, contendibilità ed innovazione nei mercati in cui operano o su cui esprimono un'influenza, anche indiretta, il DMA potenzia il diritto alla portabilità dei dati forniti o generati dall'utente finale nell'uso della piattaforma. A tal fine, si afferma che i dati dovrebbero essere ricevuti in un formato immediatamente ed effettivamente accessibile e utilizzabile da parte dell'utente

[91] In generale si veda P. Baschenhof, *The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?*, in *U. Ill. J.L. Tech. & Pol'y*, 2022, p. 5 ss.; A.C. Witt, *The digital markets act - regulating the wild west*, in *Common Market Law Review*, 2023, p. 625 ss.; J.U. Franck e M. Peitz, *The digital markets act and the whack-a-mole challenge*, in *Common Market Law Review*, 2024, p. 299 ss.

[92] Per una esaustiva disamina v. P. Baschenhof, *The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?*, cit., p. 16 ss.

ISBN 978-88-495-5568-4

finale o dei pertinenti terzi autorizzati dall'utente finale a cui i dati sono trasferiti, in modo tale che questi possano essere trasferiti liberamente in maniera continua e in tempo reale[93].

Il citato considerando rimarca esplicitamente come l'obbligo del *gatekeeper* di garantire l'effettiva portabilità dei dati a norma del DMA integri il diritto alla portabilità dei dati previsto dall'art. 20 GDPR. Il riferimento al GDPR è emblematico: per un verso, il DMA si pone nel solco del diritto già riconosciuto e tutelato a favore delle persone fisiche interessati con riguardo alle proprie informazioni personali. Per altro verso, il menzionato art. 6 vi apporta almeno tre rilevanti complementi: ne amplia, sul piano soggettivo, l'attribuzione agli utenti commerciali; colma, sul versante delle modalità di accesso, le carenze ancora presenti nel tessuto dell'art. 20 GDPR, prevendendo una portabilità costante, in *real time*, in linea con la logica seguita anche dal DA. Ancora, in relazione all'oggetto, diversamente dall'art. 20 GDPR la disposizione non opera una distinzione di regime normativo in ragione della natura personale o non personale, né circoscrive la sua estensione ai dati personali forniti dalla persona fisica al titolare del trattamento: il DMA prevede, infatti, la portabilità anche ai dati forniti ed anche *generati* dalle attività svolte sulla piattaforma sia dagli utenti finali sia dagli utenti commerciali. Tale allargamento ai *generated data* appare di non poco momento poiché irrobustisce il ruolo e le potenzialità del diritto alla portabilità: il quale non si limita più a facilitare la possibilità degli utenti di trasferire una "copia" dei dati da loro stessi forniti, bensì si volge a includere anche la trasmissibilità di informazioni che gli utenti altrimenti non potrebbero replicare e fornire ad altri *provider*, in quanto generati per il tramite della fruizione e interazione con i servizi digitali prestati dalle piattaforme.

Con specifico riguardo agli utenti commerciali, il § 10 dell'art. 6 DMA prescrive che il *gatekeeper* fornisca, su loro richiesta, a terzi dati aggregati e non aggregati, compresi i dati personali, forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base da parte di tali utenti commerciali e degli utenti finali che si avvalgono di prodotti o servizi prestati da tali utenti commerciali. Quanto al *quomodo*, si stabiliscono criteri più stringenti che mirano a garantire un accesso efficace, di elevata qualità, continuo e in tempo reale, oltre che a titolo gratuito. Qualora si tratti di dati personali, si prevede che il *gatekeeper* sia tenuto a fornire l'accesso nel caso in cui gli utenti finali abbiano espresso il loro consenso: qui il legislatore avrebbe dovuto, più correttamente, far riferimento alla persona fisica interessata a mente del GDPR, e non genericamente all'utente finale.

Se il DA, così come il GDPR, guarda essenzialmente alla condivisione su

[93] Sul punto Tombal e Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?*, cit., p. 17 ss.

 ISBN 978-88-495-5568-4

base volontaria, scaturente cioè dall'atto di esercizio del diritto dell'utente e/o dell'interessato, il DMA volge l'attenzione anche al diverso scenario nel quale la condivisione dei dati prescinda o superi siffatta iniziativa del privato ma sia comunque reputata necessaria dal legislatore, per il perseguimento di finalità generali di natura concorrenziale[94]. In questa prospettiva, il DMA prevede, altresì, la condivisione dei dati di ricerca, raccolti e generati dai *gatekeepers* di questi servizi, anche al di là dell'esercizio del potere da parte dell'interessato o degli utenti: all'art. 6, § 11, impone ai *gatekeepers* di trasmettere a qualsiasi prestatore terzo di motori di ricerca *online* "l'accesso a condizioni eque, ragionevoli e non discriminatorie ai dati relativi a classifiche, interrogazioni, clic e visualizzazioni". La *ratio* di questo obbligo si lega all'idea che l'accesso ai dati di ricerca costituisca "un'importante barriera all'ingresso e all'espansione, che mina la contendibilità dei servizi dei motori di ricerca online" (considerando 61). In quest'ottica, le istanze di accesso e portabilità dei dati su iniziativa privata non sono ritenute dal legislatore europeo uno strumento sufficiente a stimolare la concorrenza sul mercato dei motori di ricerca e su quelli ad esso correlati o dipendenti. La strategia regolatoria va oltre la logica relazionale della portabilità dei dati del GDPR e dei diritti di accesso e condivisione del DA, imponendo una misura ancor più invasiva della libertà di impresa del *gatekeeper*, mirante a perseguire il *telos* della competitività e contendibilità dei mercati digitali[95].

Tuttavia, si staglia un problema di coerenza di tale previsione e tenuta del sistema di tutela dei dati personali congegnato dal GDPR, dal momento che gli interessati non esercitano alcun controllo su tale condivisione dei dati di ricerca. Vero è che l'art. 6, § 11, del DMA subordina l'accesso a tali informazioni alla loro "anonimizzazione" quando si tratti di dati personali. Tuttavia, è noto che sul piano tecnologico sia possibile per dati personali precedentemente anonimizzati essere a un certo punto "de-anonimizzati"[96]. In seno ai considerando del DMA, il legislatore europeo si limita a identificare questo aspetto di criticità richiedendo al *gatekeeper* di "garantire la protezione dei dati personali degli utenti finali, anche contro eventuali rischi di "reidentificazione", con mezzi appropriati, come l'anonimizzazione di tali dati personali, senza degradare in modo sostanziale la qualità dei dati stessi" (considerando 61). Nondimeno, anche per la condivisione e l'utilizzo dei dati di ricerca da parte di terzi devono trovare applicazione i principi generali di limitazione delle finalità e di minimizzazione dei dati di cui all'art. 5 del GDPR.

[94] *Ibidem*, p. 19.

[95] Cfr. I. Graef, T. Petročnik e T. Tombal, *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, cit., p. 13 ss.

[96] Cfr. Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 2014, p. 6 ss.

ISBN 978-88-495-5568-4

7. La riflessione condotta dischiude all'interprete una complessa opera di coordinamento e messa a sistema di un materiale normativo estremamente frastagliato, nel quale si agitano istanze valoriali diverse e, sovente, contrapposte.

L'analisi dell'ingente produzione normativa europea più recente, chiamata a governare il mercato europeo dei dati, mostra l'avanzare di alcune traiettorie evolutive fondamentali. Anzitutto, la moltiplicazione dei diritti di accesso e portabilità e degli obblighi di messa a disposizione dà forma al nuovo paradigma della *condivisione* dei dati nelle relazioni di mercato: ciò si apprezza tanto sul piano dell'ampliamento dell'oggetto di tali situazioni soggettive, che si appuntano sui dati in quanto tali, quale che ne sia la natura (personale o non personale) e la fonte (forniti o generati); quanto della dilatazione dei soggetti titolari di siffatte prerogative e facoltà, non più esclusivamente riferite alla persona fisica interessata come nel diritto alla portabilità previsto dall'art. 20 del GDPR, bensì estese ad altri potenziali attori (persone fisiche e giuridiche, utenti finali e commerciali, *data holder* e *data recipients*). In questo rinnovato modello, l'interesse alla circolazione, allo scambio, all'accesso e alla condivisione dei dati tende a concorrere e, sovente, a prevalere sulle situazioni di privativa, di controllo e di protezione. L'idea di politica del diritto sottesa è che i dati rappresentino essenziali fattori della produzione per i mercati digitali e dei beni interconnessi, catalizzatori di concorrenza e innovazione, dei quali è necessario incentivare, favorire e financo imporre il più possibile la *disclosure* e lo *sharing*.

In questa prospettiva, appare inevitabile il progressivo appannamento della distinzione tra dati personali e non personali e la contestuale ascesa della categoria del dato *tout court*. Le pratiche di condivisione volontaria del DGA, i diritti di accesso e condivisione dei dati e gli obblighi di messa disposizione dettati dal DA, così come i diritti di portabilità dei dati generati dagli utenti delle *digital platforms* e l'obbligo per i *gatekeeper* di condividere l'accesso ai dati di ricerca previsti dal DMA contrassegnano una visione olistica del legislatore europeo, per la quale la *divisio* tra dati personali e non personali non appare più dirimente nel definire portata, contenuto e scopi degli strumenti di condivisione. In ottica schiettamente concorrenziale, l'introduzione di regole comuni alla circolazione dei dati, quale che ne sia la natura, appare più efficiente poiché tende ad avvicinare il diritto positivo alla realtà dei mercati da regolare, ove questa partizione non sempre esprime un significativo rilievo sul piano dei processi di estrazione di valore dai dati necessari a stimolare la concorrenza, la contendibilità e l'innovazione sui mercati digitali e dei beni tecnologicamente più all'avanguardia[97].

[97] Peraltro, con una singolare eterogenesi dai fini, il baluardo della natura personale dei dati viene sollevato proprio dai titolari dei dati e dalle grandi piattaforme digitali come argomento – ammantato da artefatte esigenze di protezione dei dati personali degli utenti –

 ISBN 978-88-495-5568-4

In terzo luogo, sul piano dogmatico, si staglia all'orizzonte la configurabilità di un modello di dogmatizzazione fondato sulla *coesistenza* di una batteria di diritti che consentono l'accesso e lo sfruttamento dei dati, intestati a più soggetti facenti parte, a vario titolo, del processo di estrazione di valore economico, ciascuno secondo la posizione, il contributo e l'interesse vantato verso quei dati[98]. In altri termini, si assiste alla *moltiplicazione* delle situazioni soggettive vertenti sui dati, corrispondenti a pretese, poteri, contenuti e interessi tra loro spesso distanti e, talora, conflittuali. I poteri di controllo riconosciuti sui dati personali all'interessato si trovano a convivere con il diritto all'accesso, all'uso e alla condivisione dei dati attribuito all'utente del prodotto e della piattaforma. Sul medesimo dato – indifferente la sua natura personale o non personale – risultano convergenti diritti di accesso, di godimento, di portabilità e condivisione ed anche di partecipazione in una quota del profitto che pertengono ai diversi soggetti coinvolti nella *value chain* di sfruttamento del dato, in funzione dell'attività di generazione, raccolta, analisi, profilazione e condivisione rispettivamente posta in essere[99].

per mantenere un vantaggio competitivo e non innescare flussi di condivisione dei dataset nella loro disponibilità (ad esempio, nel contesto della condivisione dei dati di ricerca) o per ottenere condizioni particolarmente vantaggiose per l'accesso ai dati da parte di terzi (ad esempio, nel contesto delle trattative contrattuali con il data recipient nel contesto del DA). Cfr. Tombal e Graef, *The regulation of access to personal and non-personal data in the EU: from bits and pieces to a system?*, cit., p. 19.

[98] *Mutatis mutandis* lo schema dogmatico di riferimento può essere offerto dal famoso caso statunitense *Moore* del 1990 (cfr. *Moore v. Regents*, 51 Cal. 3d 120, 271 Cal. Rptr. 146, 79, 1990), con riferimento al riconoscimento al soggetto della titolarità dei diritti di proprietà sul proprio corpo e sulle sue parti, segnatamente sulla sua milza contenente una linea cellulare particolarmente rara, mentre si è riconosciuto il diritto di brevetto a coloro che avevano derivato nuove invenzioni dallo studio delle linee cellulari generate dalla milza del signor *Moore*. Su questi aspetti cfr. G. Resta, *Towards a unified regime of data-rights?*, cit., p. 650; D.E. Winickoff e R.N. Winickoff, *The charitable trust as a model for genomic biobanks*, in *New Engl. J. Med.*, 2003, pp. 1180-1184. In tema si veda diffusamente M.C. Venuti, *Gli atti di disposizione del corpo*, Milano, 2002.

[99] In questa direzione puntano decisamente i *Principles for a Data Economy Ali-Eli* (approvati congiuntamente dall'*American Law Institute e dall'European Law Institute*, pubblicati nella loro versione definitiva il 27 settembre 2021, consultabili sul sito *https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/data-economy*) che invero non operano distinzione di sorta tra dati personali e non personali, nell'ambito della individuazione del novero dei cd. "*data rights*" (i quali comprendono, tra gli altri, il diritto di accesso e portabilità, il diritto di correzione dei dati nonché il peculiare diritto di partecipazione in una quota del profitto ricavato dall'operatore economico a fronte delle attività di sfruttamento del dato: Principle 16) si mette a punto l'innovativa categoria dei cd. "*Data Rights with Regard to Co-Generated Data*" (Principles 18-23): un denominatore comune di questi diritti è che trovano la loro giustificazione nella quota che una parte aveva nella generazione delle informazioni in gioco. In via esemplificativa, un individuo può partecipare alla generazione dei dati essendo il soggetto delle informazioni codificate, o essendo titolare o gestore di un qualcosa che è oggetto dei dati, o fornendo in altro modo un contributo alla generazione dei medesimi.

ISBN 978-88-495-5568-4

In tale modello, dunque, il profilo dell'accesso e del godimento risulta prevalente rispetto a quello della titolarità e dell'appartenenza, tanto per la natura intrinseca del bene giuridico sottostante – ossia l'informazione condensata nel dato digitale – tanto per la conformazione normativa impressa dal legislatore europeo che vuol rendere i dati suscettibili di utilizzi e riutilizzi ripetuti e per differenti scopi, motore della concorrenza, dell'innovazione e della contendibilità dei mercati digitali. In questo ambito, il punto di riferimento dogmatico non può essere rappresentato, pertanto, dallo stilema proprietario, dal paradigma dell'appartenenza dominicale, di stampo protezionistico teso cioè primariamente ad escludere gli altri dal godimento dei beni che ne formano l'oggetto[100]. Prendono vita, all'opposto,

[100] La prospettiva di indagine privilegiata in dottrina in ordine ai rapporti tra dati personali e mercato è tradizionalmente quella di carattere dominicale, concernente cioè l'inquadramento dei dati e delle informazioni personali nella categoria dei beni immateriali suscettibili diritti di proprietà o di appartenenza in senso lato. In Europa, l'interesse verso la "proprietarizzazione" delle informazioni personali nasce certamente in Francia con le tesi di P. Català, *Ebauche d'une théorie de l'information*, cit., pp. 26-27, il quale riconosceva nei diritti della persona interessata "des prerogatives relevant du droit réel", concludendo che la protezione accordata agli individui rifletteva un diritto sui dati personali piuttosto che un diritto a questo tipo di informazione. Nella più recente dottrina francese ritornano sul tema S. Gutwirth e G. González Fuster, *L'éternel retour de la propriété des données: de l'insistance d'un mot d'ordre*, in *Law, norms and freedoms in cyberspace - Liber amicorum Yves Poullet*, a cura di Degrave-de Terwangne-Dusollier-Queck, Bruxelles 2018, p. 117 ss.; A. Strowel, *Les données: des ressources en quête de propriété. Regards sur quelques développem, ivi*, p. 251 ss. Qui si registra lo slogan *Mes data sont à moi*, coniato da un *think tank* francese di impostazione liberista vicino al partito En Marche (lo riferisce J. Drexl, *Legal challenges of changing role of personal data and non-personal data in the data economy*, cit., 2019, p. 9). La recente ripresa del dibattito, sotto forma del riconoscimento della cd. data ownership, proviene in particolare dalents récents en droit européen la dottrina tedesca e olandese. Diversi autori difendono la tesi per cui dei dati personali possa predicarsi una vera e propria appartenenza di stampo proprietario: F. Hofmann, *"Absolute Rechte" an Daten - immaterialgüterrechtliche Perspektive*, in *Rechte an Daten*, cit., p. 9 ss.; T. Hoeren, *Dateneigentum und Datenbesitz, ivi*, p. 37 ss.; V. Janecek, *Ownership of personal data in the Internet of Things*, in *Computer Law & Security Review*, 2017, p. 1039 ss.; H. Zech, Information as property, cit., p. 192 ss.; C. Berger, *Property Rights to Personal Data? An Exploration of Commercial Data Law*, in *Zeitschrift für geistiges Eigentum*, 2017, p. 340; E. Tjong Tjin Tai, *Data ownership and consumer protection*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2018, p. 136 ss. Rispetto a queste posizioni è drastico il condivisibile giudizio negativo di V. Zeno Zencovich, *Dati, grandi dati, dati granulari*, in *Riv. dir. media*, 2018, p. 4; Id., *Do "Data Markets" exist?*, cit., p. 25, ove scrive che «*trying to assert an "ownership" over one's personal data is an attempt that (in continental Europe) not only totally ignores over 150 years of debate on personality rights (von Gierke's and Kohler's contributions being the starting point), but even forgets the roots of continental legal systems: 'Dominus membrorum suorum nemo videtur'*». Più in generale nella riflessione europea: cfr. N. Purtova, *Property rights in personal data: A European perspective*, The Hague, 2011; Ead., *Property rights in personal data*; nonché i saggi raccolti nel volume curato da S. Lohsse, R. Schulze e D. Staudenmayer, *Trading Data in the Digital*

 ISBN 978-88-495-5568-4

categorie dogmatiche e situazioni soggettive che formalizzano gli interessi all'accesso, alla disponibilità, alla compartecipazione e alla condivisione[101].

Uno sguardo d'insieme su queste tendenze evolutive avverte del sottile, ma irresistibile, *scivolamento* della logica sottesa alla disciplina dei dati: non più costitutivamente protesa volta a precostituire un meccanismo di salvaguardia di determinati beni incorporali in ragione della loro immediata inerenza all'individuo e alla conoscenza di aspetti essenziali della sua personalità; bensì precipuamente volta a fissare un sistema di regole che governa la circolazione e l'uso di dati in relazione alla loro strutturazione formale di ordine tecnologico (e, segnatamente, la leggibilità da un sistema automatizzato), indipendentemente dal tipo di significati e contenuti (personali o meno) che questi siano atti a veicolare[102]. Seguendo un moto pendolare teleologico e assiologico, l'impianto normativo trascorre, cioè, dal polo del controllo e della protezione agli antipodi dell'accesso e della

Economy: Legal Concepts and Tools, cit., ed in particolare gli scritti di P.B. Hugenholtz, *Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?*, cit., p. 75; D. Zimmer, *Property rights regarding data*, cit., p. 101 ss.; F. Mezzanotte, Access to Data: The Role of Consent and the Licensing Scheme, p. 159. Nella letteratura italiana si veda L.C. Ubertazzi, *I diritti d'autore e connessi. Scritti*, Milano, 2003, p. 145 ss.; Id., *Proprietà intellettuale e privacy*, in *Aida*, 2014, p. 435 ss., che, dalla prospettiva della tutela autoriale, si esprime a favore della qualificazione dell'informazione di carattere personale come un bene immateriale, di cui è predicabile l'assoggettamento al diritto della proprietà intellettuale. Sul tema, con differenti opinioni, cfr. P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ*., 1990, p. 326 ss.; G. De Nova, *I nuovi beni come categoria giuridica*, in *Dalle res alle new properties*, Milano, 1991, p. 15; R. Pardolesi e C. Motti, *L'informazione come bene, ivi*, p. 37 ss.; V. Zeno Zencovich, *Informazione (profili civilistici)*, in *Digesto disc. priv., Sez. civ*., Torino, 1993, p. 420 ss.; Id., *Sull'informazione come «bene» (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv*., 1999, p. 485 ss. Nella letteratura statunitense, che si muove in un filone di riflessione più ampio che coinvolge i rapporti tra privacy e property, nelle accezioni peculiari della cultura giuridica americana cfr. per tutti V. Bergelson, *It's Personal But is it Mine? Toward Property Rights in Personal Information*, in *University of California Davis Law Review*, 2003, pp. 379-451; L. Lessig, *"Privacy as property"*, in *Social Research,* 2002, pp. 247- 269; P. Samuelson, *'Privacy as Intellectual Property?'*, in *Stanford Law Review,* 2000, pp. 1125-1173; R. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 1996, pp. 2381-2417; K.C. Laudon, *Markets and Privacy*, in *Communications of the ACM*, 1996, pp. 92-104.

[101] In questa direzione si muove anche G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 610; Id., *Towards a unified regime of data-rights?,* cit., p. 655; nonché Drexl, *Designing Competitive Markets for Industrial Data. Between Propertisation and Access*, cit., 273; Mezzanotte, *Access to Data: The Role of Consent and the Licensing Scheme*, cit., p. 167.

[102] Si veda sul punto B. Steinrötter, *Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts,* in *RDI*, 2021, p. 481; F. Rosenkranz e M. Scheufen, *Die Lizenzierung von nicht-personenbezogenen Daten. Eine rechtliche und rechtsökonomische Analyse*, in *ZfDR*, 2022, p. 168; H. Richter e P.R. Slowinski, *The Data Sharing Economy: On the Emergence of new Intermediaries*, 2019, p 4 ss.; H. Schweitzer e M. Peitz, *Ein neuer europäischer Ordnungsrahmen für Datenmärkte?*, in *NJW*, 2018, pp. 279-280.

ISBN 978-88-495-5568-4

condivisione, nel segno pieno della mercificazione e della libera circolazione dei dati, anche personali, volta a innescare effetti procompetitivi sui mercati che, attorno ad essi, costruiscono il proprio piano cartesiano.

Questo spostamento dell'asse normativo ripropone all'attenzione del civilista il tema della (im)possibile convivenza dei due *esprit*, quella personalistico e quella mercantilistico, che innervano la regolamentazione dei dati[103]. Dinanzi alla contraddizione di fondo che emerge tra la normativa di *Datenschutz*, la quale tende a sottrarre i dati al mercato, e il nuovo *corpus* normativo che, seguendo le logiche della concorrenza, stimola l'espansione capillare e sistematica del mercato dei dati, il punto archimedeo potrebbe esser in futuro rappresentato dalla valorizzazione della natura "multidimensionale" dell'autodeterminazione del singolo in questa materia, che esalti la componente *relazionale* e *collettiva* delle scelte individuali concernenti il trattamento dei dati personali di cui il nuovo paradigma dell'accesso e della condivisione si fa latore[104]. In questa prospettiva, un ruolo centrale saranno chiamate a svolgere le "cooperative di dati"[105], quale prototipo dei prestatori di servizi di intermediazione dei dati introdotti dal DGA: al considerando 31 si legge come esse siano destinate a "rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati", in modo da offrire scelte migliori ai singoli membri del gruppo o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo[106]. La funzione attribuita alle cooperative di dati dal legislatore europeo è e resta, allo stato attuale, di na-

[103] C. Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy*, in *Trading Data in the Digital Economy: Legal Concepts and Tools*, cit., pp 327-356.

[104] In letteratura riflessioni in questa prospettiva sono impostate da S. Viljoen, *A Relational Theory of Data Governance*, in *Yale L. J.*, 131, 573, 202; Y. Braudo-Bahat, *Towards a relational conceptualization of the right to personal autonomy*, in *American University Journal of Gender, Social Policy & the Law*, 2017, pp. 111-154; I. Graef, T. Petročnik e T. Tombal, *Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice*, cit., spec. p. 9 ss.

[105] Cfr. E. Bietti e A. Etxeberria, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, in *White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman KleinCenter for Internet & Society Research Sprint*, 2021, accessibile all'indirizzo *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*.

[106] Si veda quanto disposto dall'art. 12, § 1, lett. m), DGA, nel delineare i doveri fiduciari dell'intermediario dei dati personali (e segnatamente delle cooperative) nel rapporto con gli interessati: "il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso".

 ISBN 978-88-495-5568-4

tura puramente assistenziale e consulenziale a favore dei singoli, precedente e prodromica alla manifestazione del consenso, che permane atto personalissimo dell'interessato: la disciplina non si spinge, infatti, a contemplare fattispecie di sostituzione in senso tecnico sotto forma di rappresentanza dei singoli componenti, come sembra indicare l'inciso dello stesso considerando 31 per il quale "i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi"[107]. L'emersione di questa figura pare, tuttavia, aprire una breccia nella lettura tradizionale rigidamente individualistica della disciplina di protezione dei dati personali, assisa sul *totem* del consenso, e schiudere nuovi spazi e funzioni all'autonomia contrattuale nella condivisione e circolazione dei dati sul mercato riguardata nella dimensione relazionale dell'impatto su altri interessi individuali, collettivi e generali.

[107] Sul punto G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., pp. 626-627.

ISBN 978-88-495-5568-4

Giuseppe Versaci

La regolazione dei dati per l'agricoltura di precisione tra questioni generali ed esigenze settoriali

Sommario: 1. Agricoltura di precisione e qualificazione dei dati rilevanti. – 2. La circolazione dei dati in assenza di un diritto di proprietà: l'impianto del *Data Act*. – 3. La condivisione dei dati in ambito agricolo: sfiducia, abusi e iniziative auto-regolatorie. – 4. L'adattamento del *Data Act* alle peculiarità del settore agricolo: prospettive future.

1. La Commissione europea, nella Comunicazione del febbraio 2020 intitolata «Una strategia europea per i dati», tra i vari aspetti esaminati, ha affermato: «I dati sono uno degli elementi essenziali ai fini del rafforzamento della sostenibilità, del rendimento e della competitività del settore agricolo. L'elaborazione e l'analisi dei dati relativi alla produzione, in particolare in combinazione con altri dati sulla catena di approvvigionamento e con dati di altro tipo, quali i dati dell'osservazione terrestre o i dati meteorologici, rendono possibile l'applicazione precisa e mirata di approcci produttivi a livello di azienda agricola»[1].

Una tale dichiarazione è emblematica di quanto l'economia dei dati sia (divenuta) trasversale, non limitandosi ad incidere – al contrario di come si potrebbe pensare – solo nel settore dei servizi e in quello industriale, vista la notevole rilevanza assunta anche nel settore primario per antonomasia, qual è quello agricolo, oggetto d'esame in questa sede[2]. Tuttavia, discorrere genericamente del valore dei dati nelle più svariate attività economiche rischia di risultare ormai un truismo, che non aiuta a inquadrare correttamente i problemi giuridici sottesi alle trasformazioni dettate dalle innovazioni tecnologiche. Occorre, dunque, chiarire in primo luogo quali sono i dati al centro della c.d. "agricoltura di precisione"[3], soffermandosi sulle caratteristiche e le modalità di sfruttamento degli stessi.

[1] Commissione europea, Una strategia europea per i dati, COM(2020) 66 final, p. 35.

[2] Per un'ampia panoramica delle trasformazioni in atto nella filiera agroalimentare, v. M. Ferrari, *Fattori di produzione, innovazione e distribuzione di valore nella filiera agroalimentare*, Milano, 2023.

[3] L'agricoltura di precisione è definita come una forma di gestione dell'impresa agricola caratterizzata dall'utilizzo di tecnologie digitali per monitorare e ottimizzare i processi di produzione: così M. Kritikos, *Precision agriculture in Europe: Legal, social and ethical considerations*, Bruxelles, 2017, p. 1.

 ISBN 978-88-495-5568-4

I dati – cioè, le informazioni in formato digitale – cui ci si riferisce, a ben vedere, coincidono in gran parte con le informazioni che da sempre rivestono importanza per il settore agricolo: quelle sui componenti del suolo, sulle condizioni ambientali, sulla salute degli animali, sui raccolti, ecc.[4]. Mentre, un tempo, tali informazioni erano oggetto di rilevazione empirica da parte degli agricoltori e, negli ultimi decenni, sono state oggetto di rudimentali rilevazioni automatizzate tramite i primi ausili tecnologici, oggi i medesimi dati sono raccolti, in termini molto più dettagliati oltre che in tempo reale, da dispositivi sofisticati (ad es., droni o robot intelligenti[5]), capaci di archiviarli ed elaborarli digitalmente, anche attraverso la combinazione con altri dati raccolti dagli stessi o da altri dispositivi[6], al fine di suggerire agli agricoltori l'adozione di misure di precisione (ad es., per l'irrigazione, la fertilizzazione, la semina), che mirano alle specifiche esigenze di un determinato terreno o prodotto agricolo, così da rendere non solo più efficienti i processi della filiera produttiva, ma anche più sostenibile, a livello ambientale, la stessa produzione[7].

Nell'ambito di tali operazioni, si è soliti distinguere i dati che sono generati e/o raccolti dai nuovi dispositivi tecnologici – c.d. dati-*input*, o "*primary data*" – dai dati che costituiscono il risultato dell'elaborazione compiuta dagli algoritmi incorporati negli stessi o da altri dispositivi – c.d. dati-*output* o "*computed data*"[8], il cui valore è certamente superiore ai primi[9]. Di là da tale distinzione, basilare nel fenomeno dei *Big Data*, il legame che l'imprenditore agricolo instaura coi dati (rilevanti per l'agricoltura di precisione) può essere differenziato sotto un altro profilo. Invero, sulla base di come si presentano i flussi dei dati, si è proposto di definire "localizzati" i dati che vengono generati e/o raccolti all'interno dell'azienda agricola affinché sia-

[4] Cfr. S. van der Burg *et al.*, *Ethics of smart farming: Current questions and directions for responsible innovation towards the future*, in *NJAS - Wageningen Journal of Life Sciences*, 2019, 90-91, p. 3.

[5] La letteratura giuridica in ordine ai problemi posti dall'intelligenza artificiale è diventata sterminata negli ultimi anni: per uno sguardo ampio, attento alle questioni di carattere non solo civilistico, v. G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ.*, 2021, p. 823 ss.

[6] Non è certo una novità ormai che, in base al fenomeno dei *Big Data*, più dati si riescono a raccogliere ed elaborare, facendo ricorso a sorgenti diverse e a sistemi di calcolo sempre più veloci, maggiore sarà il valore dell'informazione che se ne ricava. Per una panoramica delle ricadute applicative nell'ambito delle imprese agricole, v. S. Wolfert *et al.*, *Big Data in Smart Farming - A review*, in *Agricultural Systems*, 2017, p. 69 ss.

[7] Sul rapporto tra agricoltura di precisione e sostenibilità ambientale, v. *Camera dei deputati, Agricoltura di precisione, Servizio Studi, XVIII Legislatura*, 25 luglio 2022.

[8] Cfr. S. van der Burg *et al.*, *Ethics of smart farming*, cit., p. 4.

[9] Sul diverso valore tra i "*raw data*" e i "*processed data*", cfr. C. Atik e B. Martens, *Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU*, in *JIPITEC*, 2021, p. 372.

ISBN 978-88-495-5568-4

no utilizzati per la relativa impresa (ad es., i dati sul suolo, sui fertilizzanti, sul consumo idrico), mentre i dati che, pur venendo generati e/o raccolti al di fuori dell'azienda, finiscono per essere utilizzati ed elaborati per finalità agricole sono definiti "importati" (ad es., i dati metereologici)[10].

Simili classificazioni, però, per quanto utili per descrivere e comprendere l'architettura tecnologica[11], non sembrano apportare particolari benefici sul piano della ricostruzione giuridica. A tal riguardo, infatti, è di maggior rilievo distinguere i dati, oltre che in base ai dispositivi che li generano e/o raccolgono[12], a seconda che gli stessi dati si riferiscano o meno a componenti dell'azienda agricola o ad attività della relativa impresa: un simile fattore – come si vedrà più avanti (v. *infra* § 4) – potrebbe assurgere, in combinazione con altri elementi (ad es., la finalità di utilizzo dei dati), a criterio di risoluzione di conflitti di interesse, a prescindere da chi sia l'utilizzatore del dispositivo collettore dei dati.

È indubbio, tuttavia, che le questioni giuridiche inerenti al trattamento di dati richiedano di impiegare, come primo filtro di selezione delle discipline applicabili, quello relativo alla natura personale o non dei dati in questione: la rilevanza di tale distinzione è fin troppo nota, posto che il reg. UE 2016/679 (regolamento generale sulla protezione dei dati: c.d. RGPD) si applica soltanto nelle ipotesi in cui i dati oggetto di trattamento siano personali[13].

Riferendosi per lo più ad elementi naturali come il suolo, l'acqua o le condizioni meteo, i dati necessari per l'agricoltura di precisione non sono, in genere, in grado di riguardare una persona fisica identificata o identificabile (v. art. 4, n. 1, RGPD), quale potrebbe essere il coltivatore diretto di un terreno agricolo. A supporto di tale qualificazione può richiamarsi anche il considerando 9 del reg. UE 2018/1807 (regolamento sulla libera circolazione di dati non personali), ove si menzionano «i dati sull'agricoltura di precisione» («che possono contribuire a monitorare e ottimizzare l'uso di pesticidi e acqua») proprio come possibile esempio di dati non personali. Ciò non toglie che la linea di confine tra dati personali e non è sempre piuttosto labile in quanto dipendente da elementi contestuali, che potrebbero trasformare un dato solitamente anonimo in un dato capace di riferirsi a

[10] A. Maru *et al.*, *Digital and Data-Driven Agriculture: Harnessing the Power of Data for Smallholders, Global Forum on Agricultural Research and Innovation*, Roma, 2018, p. 11 s.

[11] Id., *op. cit*., p. 14 ss.

[12] Come si dirà a breve (infra § 2), la titolarità di diritti sul dispositivo da cui i dati sono generati rileva soprattutto ai fini dell'applicazione del *Data Act*.

[13] Cfr. C. Atik, *Understanding the role of agricultural data on market power in the emerging Digital Agriculture sector: a critical analysis of the Bayer/Monsanto decision*, in D. Bosco e M.S. Gal (a cura di), *Challenges to Assumptions in Competition Law*, Cheltenham-Northampton, 2021, p. 57.

 ISBN 978-88-495-5568-4

una determinata persona fisica, e viceversa[14] (si pensi, ad esempio, ai dati che registrano i movimenti di una pianta grazie ad un sensore posto su di essa: tali dati, se combinati con altre informazioni provenienti da altre sorgenti, potrebbero talvolta fornire indicazioni circa i comportamenti tenuti dal coltivatore dell'area in questione; al contrario, i dati sui consumi idrici o sui raccolti, che si configurano come dati personali nella misura in cui l'impresa agricola sia esercitata da una persona fisica, perdono tale qualifica laddove l'esercizio dell'impresa sia imputabile ad un ente collettivo[15]).

Ad ogni modo, anche i dati *non* personali sono ormai ricompresi nell'ambito applicativo oggettivo di discipline analitiche – su tutte, il reg. UE 2023/2854 (c.d. *Data Act*)[16] e il reg. UE 2022/868 (c.d. *Data Governance Act*)[17] – che li sottraggono dal limbo giuridico in cui si trovavano fino a poco tempo fa[18]: situazione che creava notevole incertezza per gli operatori

[14] Sulla difficile demarcazione tra dati personali e non personali, v. E. Pellecchia, *Dati personali, anonimizzati, pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, p. 363 ss.; C. Wendehorst, *Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy*, in S. Lohsse, R. Schulze e D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, 2017, pp. 331-332; I. Graef, R. Gellert e M. Husovec, *Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation, TILEC Discussion Paper No*. 2018-029, 2018.

[15] Cfr. M. Kritikos, *Precision agriculture*, cit., p. 14 s.; C. Atik, *Understanding the role of agricultural data*, cit., p. 58.

[16] Per un primo commento, v. M. Eckardt e W. Kerber, *Property rights theory, bundles of rights on IoT data, and the EU Data Act,* in *Eur. J. Law Econ.*, 2024, disponibile online su: *https://doi.org/10.1007/s10657-023-09791-8* (ultima visita: 15 marzo 2024); T. Groza, *The Data Act: A Stepping Stone for a New Data Economy, Kluwer Competition Law Blog*, 15.12.2023; per diversi rilievi critici mossi nei confronti del testo della Proposta presentata dalla Commissione Europea (COM(2022) 68 final), v. W. Kerber, *Governance of IoT Data: Why the EU Data Act Will not Fulfll Its Objectives,* in *GRUR International*, 2023, p. 120 ss.; I. Graef e M. Husovec, *Seven Things to Improve in the Data Act, March 7, 2022*, disponibile online su: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793* (ultima visita: 15 marzo 2024); J. Drexl *et al.*, *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act), Max Planck Institute for Innovation and Competition Research Paper No*. 22-05, 2022, passim.

[17] Tra le prime analisi, v. G. Resta, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati,* in *Riv. trim. dir. pubbl.*, 2022, p. 979 ss.; sul testo della Proposta originaria, v. I. Graef e R. Gellert, *The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing, TILEC Discussion Paper No.* DP2021-006, March 25, 2021, disponibile online su: *https://ssrn.com/abstract=3814721* (ultima visita: 15 marzo 2024); F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act,* in *Contr. impr./Eur.*, 2021, p. 199 ss., spec. 237 ss.

[18] Cfr. G. Resta, *Towards a unified regime of data-rights? Rapport de synthèse*, in T. Pertot (a cura di), *Rechte an Daten*, Tübingen, 2020, p. 242.

ISBN 978-88-495-5568-4

economici e i soggetti pubblici coinvolti nella raccolta e nell'utilizzo di tali dati. Proprio tale incertezza circa il regime giuridico applicabile è ritenuta essere, a livello generale, una delle ragioni che hanno finora ostacolato gli scambi di dati in ambito economico, impedendo il pieno sfruttamento del potenziale che viene loro riconosciuto[19].

Invero, a fronte dell'immaterialità delle risorse di cui ci stiamo occupando, la definizione dei diritti che insistono sulle stesse diventa fondamentale non solo per la loro qualificazione come beni giuridici (in senso privatistico)[20], ma anche – e, soprattutto, in termini operativi – per l'individuazione delle regole applicabili in sede circolatoria.

2. Tra le situazioni giuridiche soggettive che possono immaginarsi, è evidente che, se si riconoscesse una proprietà sui dati, l'utilizzo degli stessi ad opera di terzi non potrebbe avvenire – almeno, in linea generale – senza il consenso del legittimo titolare, con la conseguenza di rendere giuridicamente escludibile una risorsa che, di per sé, non si presenta a livello economico come un bene privato[21]. L'attribuzione di diritti proprietari permetterebbe indubbiamente la creazione di un vero e proprio mercato dei dati, assegnando a questi ultimi un valore commerciale in ragione dei poteri che solo determinati soggetti, in un simile scenario, potrebbero esercitare sulla risorsa in questione.

Com'è noto, non è questo l'approccio che il legislatore europeo ha adottato a proposito della circolazione dei *dati personali*[22]. Di contro, il

[19] Commissione europea, *Impact Assessment Report, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), SWD(2022) 34 final*, pp. 15-17.

[20] Cfr. D. Messinetti, *Oggettività giuridica delle cose incorporali*, Milano, 1970, *passim*, spec. p. 122 ss.; O.T. Scozzafava, *I beni e le forme giuridiche di appartenenza*, Milano, 1982, p. 91 ss.; A. Gambaro, *I beni*, in *Tratt. dir. civ. comm. Cicu e Messineo*, Milano, 2012, p. 99 ss. Per quanto riguarda il principio di tipicità dei beni, v. le riflessioni critiche di A. Belfiore, *I beni e le forme giuridiche di appartenenza. A proposito di una recente indagine*, in *Riv. crit. dir. priv*., 1983, p. 920 ss.; M. Barcellona, *Attribuzione normativa e mercato nella teoria dei beni giuridici*, in *Quadrimestre*, 1987, p. 613 s.

[21] Sull'assenza di caratteristiche ontologiche che rendano un bene necessariamente escludibile o non escludibile, rivale o non rivale, comune o privato, v. F. Denozza, *Dalla tragedia dei (falsi) commons, al dramma del bail in*, 25 marzo 2016, disponibile online su: *https://www.casadellacultura.it/375/parliamo-di-beni-comuni* (ultima visita: 15 marzo 2024).

[22] Tra i molti, v. di recente V. Bachelet, *Il consenso oltre il consenso. Dati personali, contratto, mercato*, Pisa, 2023, p. 103 ss., cui si rinvia per gli ulteriori riferimenti bibliografici; con un taglio principalmente comparatistico, v. G. Alpa, *La "proprietà" dei dati personali*, in M. D'Auria (a cura di), *I problemi dell'informazione nel diritto civile, oggi. Sudi in onore di Vincenzo Cuffaro*, Roma, 2022, p. 35 ss.; sulla pluralità di situazioni giuridiche soggettive che insistono sui dati personali, v. C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, p. 12 s.

 ISBN 978-88-495-5568-4

riconoscimento di un diritto di proprietà è stato recentemente al centro del dibattito giuseconomico (principalmente di area tedesca) riguardante la regolazione dei *dati non personali*: nello specifico, si è proposto di attribuire un simile diritto al "produttore" di tali dati, individuato nell'utilizzatore qualificato del dispositivo tecnologico da cui i dati vengono generati[23]. L'idea originaria, alla base della proposta formulata in dottrina, non era tanto quella di attribuire maggiori poteri difensivi ai produttori di dati, quanto piuttosto quella di favorire gli scambi in ragione, da un lato, dell'incentivo remunerativo connesso all'atto dispositivo e, dall'altro, della maggiore chiarezza che il concetto di proprietà avrebbe potuto fornire agli operatori economici[24].

Sebbene tale proposta sia stata inizialmente presa in considerazione dalla Commissione europea[25], dopo poco tempo è stata accantonata nel percorso regolatorio che ha preceduto l'approvazione del *Data Act*[26], il cui considerando 6, nel ritenere preferibile adottare un approccio impostato sull'*accesso* ai dati «rispetto alla concessione di diritti esclusivi», certifica il totale abbandono del paradigma dominicale.

A far propendere per tale decisione pesano vari argomenti. Anzitutto, si è evidenziato come l'introduzione di un diritto esclusivo su una risorsa immateriale si giustifichi – a livello economico – quando serve un incentivo alla produzione di tale risorsa, così come avviene per i diritti di proprietà intellettuale ed industriale: nel caso dei dati *grezzi*, invero, non occorre un simile incentivo, posto che il loro livello di produzione è già sufficientemente elevato[27]. Inoltre, anche l'idea secondo la quale, grazie alla proprietà sui dati, gli scambi sarebbero favoriti dalla riduzione dei costi di transazione è stata criticata per la mancanza di analisi empiriche che dimostrino

[23] La proposta è stata avanzata da H. Zech, *Data as a tradeable commodity*, in A. De Franceschi (a cura di), *European contract law and the digital single market. The implications of the Digital Revolution*, Cambridge, 2016, p. 74 ss.

[24] Id., *op. ult. cit*., p. 77 s. Cfr. Commissione europea, *Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final*, p. 33, ove si considera la proposta relativa alla «*creation of a new data producer right with the objective of enhancing the tradability of non-personal or anonymised machine-generated data as an economic good*».

[25] Commissione europea, *Costruire un'economia dei dati europea, COM(2017) 9 final*, p. 13.

[26] Già nella Comunicazione della Commissione europea, "*Una strategia europea per i dati*", cit., è scomparso qualsiasi riferimento alla proposta di introdurre diritti proprietari sui dati.

[27] W. Kerber, *Rights on Data: The EU Communication 'Building a European Data Economy' from an Economic Perspective*, in S. Lohsse, R. Schulze e D. Staudenmayer (a cura di), *Trading Data in the Digital Economy: Legal Concepts and Tools*, Baden-Baden, 2017, p. 116 ss.; J. Drexl, *Designing Competitive Markets for Industrial Data - Between Propertisation and Access*, in *JIPITEC*, 2017, p. 273.

ISBN 978-88-495-5568-4

tale effetto[28]. E ancora, un ulteriore elemento critico – forse il principale, sul piano dell'analisi economica – è rappresentato dalla circostanza che i diritti proprietari potrebbero finire per consolidare le posizioni di forza di chi attualmente detiene il controllo, in via fattuale, di grandi volumi di dati, con il risultato di ostacolare ancor di più la condivisione degli stessi nel mercato[29]. Ad ogni modo, di là dagli argomenti di carattere strettamente economico, non può negarsi che la logica proprietaria si scontrerebbe altresì con interessi rilevanti sul piano pubblicistico[30]: basti pensare, a titolo puramente esemplificativo, all'uso dei dati per la ricerca scientifica.

In virtù delle suddette obiezioni, il modello proprietario non risulta congeniale nemmeno alla circolazione dei dati *non* personali, dove, almeno in astratto, non ricorrono i rischi (personalistici) tipici del trattamento dei dati personali[31].

Come si è anticipato, il *Data Act*, con un taglio trasversale ricomprendente qualsiasi tipologia di dato (personale e non) che consista in una «rappresentazione digitale di atti, fatti o informazioni»[32] e che risulti generato da un prodotto connesso[33] o da un servizio ad esso correlato[34], va nella direzione di attribuire a determinati soggetti – ossia, gli «utenti» dei prodotti,

[28] W. Kerber, *op. ult. cit*., p. 120.

[29] J. Drexl, *Connected devices - an unfair competition law approach to data access rights of users*, in German Federal Ministry of Justice and Consumer Protection e Max Planck Institute for Innovation and Competition (a cura di), *Data access, consumer interests and public welfare*, Baden-Baden, 2021, p. 495.

[30] Cfr. P.B. Hugenholtz, *Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?*, in S. Lohsse, R. Schulze e D. Staudenmayer (a cura di), *Trading Data*, cit., p. 94 ss.; E. Cremona, *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso,* in *Riv. it. inform. dir.,* 2023, p. 112 ss., spec. 124 ss.

[31] Tuttavia, sulla retorica personalistica che ha caratterizzato, talvolta in modo eccessivo, il trattamento dei dati personali, v. V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf*., 2018, p. 691 s.; Id., *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ*., 2020, pp. 642-645.

[32] Art. 2, n. 1), reg. 2023/2854, che, oltre a quanto riportato nel testo, considera "dati" pure «qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

[33] Per "prodotto connesso" si intende «un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente» (art. 2, n. 5), reg. 2023/2854).

[34] Per "servizio correlato" si intende «un servizio digitale diverso da un servizio di comunicazione elettronica, anche software, connesso con il prodotto al momento dell'acquisto, della locazione o del noleggio in modo tale che la sua assenza impedirebbe al prodotto connesso di svolgere una o più delle sue funzioni o che è successivamente connesso al prodotto dal fabbricante o da un terzo al fine di ampliare, aggiornare o adattare le funzioni del prodotto connesso» (art. 2, n. 6), reg. 2023/2854).

 ISBN 978-88-495-5568-4

o servizi correlati, generatori di dati[35] e i «destinatari dei dati», soggetti terzi indicati dagli stessi utenti[36] – diritti di accesso ai dati e di relativo utilizzo. Tale attribuzione di diritti di accesso e utilizzo è resa possibile grazie all'imputazione di una serie di obblighi legali in capo al c.d. «titolare dei dati»[37], che non è il titolare di un nuovo diritto di esclusiva avente ad oggetto i dati[38], bensì è semplicemente colui che esercita su di essi un controllo fattuale[39], a cui deve affiancare – per legittimare tale controllo – una base contrattuale con l'utente del prodotto connesso al fine di poter utilizzare i dati *non personali* generati dal dispositivo in questione[40], oltre ad una base giuridica – ai sensi dell'art. 6, RGPD – al fine di poter trattare eventuali dati *personali* generati e/o raccolti dal medesimo dispositivo[41].

Nell'architettura del *Data Act*, il titolare dei dati che legittima il proprio controllo fattuale, pur non acquistando un diritto soggettivo di cui disporre liberamente[42], assume prerogative che lo pongono al centro del reticolato normativo. Egli, infatti, se da un lato può utilizzare i dati a disposizione, dall'altro deve, nel caso in cui un utente lo richieda o una disposizione del

[35] L'utente è «una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato» (art. 2, n. 12), reg. 2023/2854).

[36] Il destinatario dei dati è «una persona fisica o giuridica, che agisce per fini connessi alla sua attività commerciale, imprenditoriale, artigianale o professionale, diversa dall'utente di un prodotto connesso o di un servizio correlato, a disposizione della quale il titolare dei dati mette i dati, e che può essere un terzo in seguito a una richiesta da parte dell'utente al titolare dei dati o conformemente a un obbligo giuridico ai sensi del diritto dell'Unione o della legislazione nazionale adottata conformemente al diritto dell'Unione» (art. 2, n. 14), reg. 2023/2854).

[37] Il titolare dei dati è «una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato» (art. 2, n. 13), reg. 2023/2854).

[38] V. considerando 5, reg. 2023/2854, ove il legislatore europeo avverte che «[è] opportuno non interpretare il presente regolamento come un atto che riconosce o conferisce ai titolari dei dati un nuovo diritto di utilizzare i dati generati dall'uso di uno prodotto connesso o di un servizio correlato». Un lessico pressoché analogo si ritrova anche nel considerando 25 del regolamento.

[39] Cfr. M. Eckardt e W. Kerber, *Property rights theory*, cit., p. 6 ss. Il controllo fattuale sui dati da parte del titolare, che solitamente (ma non per forza) è il fabbricante del prodotto da cui i dati sono generati, è ottenuto grazie al fatto che «i fabbricanti sono in grado di determinare, attraverso il controllo della progettazione tecnica dei prodotti connesso o dei servizi correlati, quali dati sono generati e le modalità per potervi accedere, anche se non hanno alcun diritto legale a tali dati» (considerando 20, reg. 2023/2854).

[40] V. considerando 25 e art. 4, § 13, reg. 2023/2854.

[41] V. considerando 7 e art. 1, § 5, reg. 2023/2854.

[42] V., oltre al considerando 25, l'art. 4, § 14, reg. 2023/2854.

ISBN 978-88-495-5568-4

diritto europeo o nazionale lo preveda, concedere ad altri soggetti – tramite la conclusione di un contratto – l'accesso alle risorse immateriali di cui ha il controllo[43]. La capacità di concludere un contratto – per quanto obbligata – denota un qualche potere dispositivo del titolare dei dati; tuttavia, l'atto di disposizione, nella trama normativa del *Data Act*, non rappresenta tanto lo strumento mediante il quale il titolare dei dati realizza (liberamente) il valore di scambio del bene, quanto piuttosto il mezzo idoneo a consentire una condivisione dei dati, da parte del titolare, con soggetti che non potrebbero altrimenti utilizzare i beni in questione[44].

Per svolgere tale funzione, il contratto tra il titolare e il destinatario dei dati risulta imposto nell'*an* (sebbene il *Data Act* non lo dica espressamente, il titolare dei dati ha sostanzialmente l'obbligo di concludere un contratto per mettere i dati a disposizione dei destinatari indicati dagli utenti[45]) e conformato nel *quid* (da un lato, il compenso per la messa a disposizione dei dati dev'essere ragionevole e non discriminatorio[46]; dall'altro, il contratto non deve contenere clausole abusive circa le modalità di messa a disposizione[47]). Di contro, secondo alcuni autori, il contratto che riguarda, a monte, il rapporto tra il titolare dei dati e l'utente del prodotto connesso, generatore dei dati, non risulta adeguatamente "conformato" a scopo regolatorio, con un ampio spazio di manovra per l'autonomia privata che potrebbe facilmente tradursi in un (abuso di) potere del titolare dei dati, in virtù della maggiore forza contrattuale, di imporre le proprie condizioni[48]. Ad avviso

[43] L'art. 8, § 1, reg. 2023/2854 prevede, infatti, che «[i]l titolare dei dati […] concorda con il destinatario dei dati le modalità della messa a disposizione dei dati e lo a condizioni eque, ragionevoli e non discriminatorie e in modo trasparente» (corsivo aggiunto), tanto che l'art. 8, § 2 e l'art. 13 del medesimo regolamento parlano di clausole contrattuali concernenti l'accesso ai dati e l'utilizzo degli stessi.

[44] Sulla rilevanza del contratto, pur in assenza di un riconoscimento di diritti proprietari sui dati, sia consentito rinviare a G. Versaci, *Note minime sulla circolazione dei dati nei rapporti tra imprese*, in *Studi e materiali*, 2022, p. 21 s.

[45] Ai sensi dell'art. 8, § 1, reg. 2023/2854, «[i]l titolare dei dati […] è tenuto a mettere i dati a disposizione di un destinatario dei dati a norma dell'articolo 5 o a norma di normative dell'Unione o nazionali applicabili adottate in conformità del diritto dell'Unione» (corsivo aggiunto).

[46] V. art. 9, § 1, reg. 2023/2854.

[47] V. art. 13, reg. 2023/2854.

[48] Lo evidenziano M. Eckardt e W. Kerber, *Property rights theory*, cit., p. 16, i quali comunque ritengono che i maggiori problemi si presentino nei rapporti (tra titolare dei dati e utente del prodotto) B-to-C, e non in quelli B-to-B; tuttavia, non ci sembra si possa escludere che l'ampia libertà contrattuale possa condurre ad un fallimento del mercato anche nei rapporti tra imprese, soprattutto quando l'impresa utente non dovesse avere alternative di mercato soddisfacenti per l'acquisto di determinati dispositivi digitali. Sul testo della proposta originaria, v. già W. Kerber, *Governance of IoT Data*, cit., p. 131 ss., critico nei confronti dell'approccio adottato dal legislatore europeo, ritenuto poco coerente rispetto agli stessi obiettivi professati dal *Data Act*.

 ISBN 978-88-495-5568-4

di chi scrive, però, tale obiezione può essere almeno in parte superata se si considera che pure le clausole contenute nel contratto tra il titolare dei dati e l'utente devono essere sottoposte a un controllo di abusività, anche quando l'utente sia un'impresa, purché – in quest'ultimo caso – le clausole da valutare siano "imposte unilateralmente" (v. considerando 28, reg. UE n. 2023/2854 e, per il concetto di imposizione unilaterale, v. art. 13, par. 6, reg. UE n. 2023/2854).

Se tale è il quadro che, a livello generale (o, se si vuole utilizzare il lessico europeo, a livello orizzontale), si è venuto a configurare, a seguito dell'emanazione del *Data Act*, in ordine alla circolazione dei dati generati da dispositivi connessi all'*Internet of Things* (c.d. *IoT data*[49]), occorre comunque segnalare che lo stesso regolamento europeo ha lasciato margini di apertura all'adozione di soluzioni diverse laddove ciò sia necessario per affrontare le specifiche esigenze di singoli settori di mercato (v. considerando 27). In particolare, in quest'ultimo considerando si è evidenziato come, nei settori caratterizzati dalla concentrazione di un piccolo numero di fabbricanti di prodotti connessi, vi possano risultare opzioni limitate a disposizione degli utenti per l'accesso, l'utilizzo e la condivisione dei dati, con la conseguenza che lo strumento contrattuale potrebbe essere insufficiente per conferire maggiori poteri agli utenti sui dati generati dai prodotti connessi che acquistano, prendono in locazione o noleggiano dai pochi fabbricanti operanti nel mercato.

Tale precisazione è particolarmente rilevante ai nostri fini in quanto, nello stesso considerando, si riporta proprio l'esempio del settore agricolo, ove la condivisione dei dati mediante contratto è stata (già) resa oggetto di un codice di condotta[50], sottoscritto da alcune importanti associazioni di categoria[51], e nulla esclude – anzi, lo stesso regolamento lo prevede espressamente – che in futuro possano essere adottate dal legislatore europeo norme speciali «per rispondere alle necessità e agli obiettivi settoriali specifici».

3. A differenza di altri ambiti, il dibattito in merito alla circolazione dei dati del comparto agricolo è molto vivace già da diversi anni[52]. In particola-

[49] Tra i molti, così vengono definiti da Id., *Governance of IoT Data*, cit., p. 120 ss.

[50] Copa, Cogeca *et al.*, *Codice di condotta UE sulla condivisione dei dati nel settore agricolo mediante un accordo contrattuale*, 2018.

[51] V. *infra* § 3.

[52] In realtà, il dibattito è particolarmente vivace tra gli operatori economici, meno tra gli studiosi di ambito giuridico, ove ancora mancano analisi approfondite, salvo alcune eccezioni: nella dottrina italiana, v. M. Ferrari, Agricoltura di precisione: proprietà o accesso?, in E. Cristiani, A. Di Lauro e E. Sirsi, *Agricoltura e Costituzione. Una Costituzione per l'agricoltura. In onore di Marco Goldoni*, Pisa, 2018, p. 223 ss.; nella dottrina europea, gli studi più avanzati sono di Can Atik: v., ad es., C. Atik, *Towards Comprehensive European Agricultural Data Governance: Moving Beyond the "Data Ownership" Debate*, in *International Review of Intellectual Property and Competition Law*, 2022, p. 701 ss.

ISBN 978-88-495-5568-4

re, in quest'ambito si ravvisano non solo i problemi comuni a tutti i settori coinvolti nell'economia dei dati, che hanno dato origine all'adozione del *Data Act* (come, ad esempio, le difficoltà di accesso ai dati e di portabilità degli stessi verso altri operatori, riscontrate dagli utenti dei dispositivi *IoT*), ma si evidenziano altresì – quanto meno, in misura maggiore rispetto ad altri settori – problemi di scarsa fiducia degli operatori di rivolgersi, già a monte, ai fornitori di prodotti e servizi tecnologici in ragione dei potenziali abusi che questi ultimi potrebbero compiere sui dati. Gli agricoltori, infatti, temono che i dati, che vengono raccolti ed elaborati dai nuovi strumenti digitali, possano essere utilizzati dagli stessi fornitori o da altri soggetti (che potrebbero ottenere i dati dai fornitori) per finalità pregiudizievoli nei loro confronti[53]: basti pensare ai dati sulla produzione agricola che potrebbero essere sfruttati, dagli operatori della grande distribuzione o dai proprietari terrieri, per alterare – a scapito degli agricoltori – i prezzi di acquisto dei prodotti o i canoni di affitto del terreno di coltivazione o allevamento[54].

Che non si tratti di preoccupazioni solo remote è dimostrato da un caso giurisprudenziale giunto all'attenzione della Corte distrettuale degli Stati Uniti per il distretto orientale dell'Oklahoma[55]. In particolare, un gruppo di allevatori di polli sosteneva che alcune imprese della filiera (nella specie, le imprese operanti nella trasformazione per la vendita della carne di pollame) avevano utilizzato, di concerto, i dati pubblicati da una società di statistica agricola – non adeguatamente anonimizzati – con lo scopo di ridurre i compensi degli allevatori cui i dati si riferivano: le condotte in questione venivano contestate sulla base delle norme in materia di concorrenza e di pratiche commerciali scorrette. La controversia sembra essersi risolta, almeno con alcune delle imprese convenute in giudizio, tramite un accordo transattivo[56].

Nello spazio economico europeo, un caso del genere avrebbe richiesto l'applicazione delle regole sulla protezione dei dati personali, laddove i dati in questione fossero stati in grado di identificare una o più persone fisiche. Tuttavia, come si è già evidenziato, non è detto che i dati relativi ad un'im-

[53] Tale mancanza di fiducia degli agricoltori è segnalata da diversi studi: L. Wiseman *et al.*, *Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming*, in *NJAS - Wageningen Journal of Life Sciences*, 2019, 90-91, p. 1 ss., *passim*; S. van der Burg *et al.*, *Trust in farm data sharing: reflections on the EU code of conduct for agricultural data sharing*, in *Ethics and Information Technology*, 2021, p. 185 s.; per ulteriori riferimenti bibliografici si rinvia ai contributi appena citati.

[54] C. Atik, *Towards Comprehensive European Agricultural Data Governance*, cit., p. 725; S. van der Burg *et al.*, *Ethics of smart farming*, cit., p. 4.

[55] Haff Poultry, Inc. *et al.* v. *Tyson Foods*, Case No. 6:17-CV-00033 (E.D. Okla.).

[56] In re: *Broiler Chicken Grower Antitrust Litigation (No. II), Long-form settlement agreement between Plaintiffs and Tyson, MDL No*. 6:20-2977-RJS-CMR, June 30, 2021; in re: *Broiler Chicken Grower Antitrust Litigation (No. II), Long-form settlement agreement between Plaintiffs and Perdue*, MDL No. 6:20-2977-RJS-CMR, August 11, 2021.

 ISBN 978-88-495-5568-4

presa agricola siano qualificabili come «personali» ai sensi dell'art. 4, n. 1, RGPD, nella misura in cui l'impresa sia esercitata da un ente collettivo. Non stupisce, allora, che gli agricoltori reclamino un maggior controllo sui dati che si riferiscono alla propria azienda, anche quando questi non siano sottoposti alle regole di protezione del reg. 2016/679, proprio per evitare di rimanere vittime di utilizzi (secondari) dei dati imprevisti e lesivi.

In questo quadro, nel 2018, su impulso dell'organizzazione di categoria più importante a livello europeo, risultante dall'unione di COPA (Comitato delle Organizzazioni Professionali Agricole convenzionali) e COGECA (Confederazione Generale delle Cooperative Agricole convenzionali), è stato adottato il già citato «Codice di condotta UE sulla condivisione dei dati nel settore agricolo mediante un accordo contrattuale», cui hanno aderito diverse organizzazioni rappresentative degli operatori della filiera agroalimentare, tra cui produttori di mangimi, pesticidi, fertilizzanti e macchinari agricoli. Come precisa lo stesso Codice, il rispetto dei principi ivi sanciti è volontario; in quest'ottica, è comunque compito dei firmatari incoraggiare «tutte le parti coinvolte nella catena agroalimentare ad allinearsi [ai] principi concordati congiuntamente»[57]. Pur con talune differenze[58], il Codice in questione sembra ispirarsi ai «*Privacy and Security Principles for Farm Data*»[59], elaborati nel 2014 (ed aggiornati da ultimo nel 2024) dall'*American Farm Bureau Federation* ponendo a fondamento l'*ownership* sui dati in capo agli agricoltori[60], i quali – in quanto titolari – possono ricorrere al contratto come strumento tipico per la condivisione dei dati con altri soggetti[61].

[57] Copa, Cogeca *et al.*, *Codice di condotta UE*, cit., p. 4.

[58] Sul punto, v. C. Atik e B. Mertens, *Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU,* in *JIPITEC*, 2021, p. 382 ss., i quali ravvisano comunque delle analogie da imputare all'influenza esercitata, in entrambi i casi, dal regolamento europeo in materia di protezione dei dati personali (ibidem). A dire il vero, però, l'RGPD non sposa un modello regolatorio improntato sulla proprietà dei dati in capo ai soggetti interessati al trattamento: v. supra § 2.

[59] American Farm Bureau Federation, *Privacy and Security Principles for Farm Data*, disponibile online su: *https://www.agdatatransparent.com/principles* (ultima visita: 15 marzo 2024).

[60] Un approccio parzialmente diverso, invece, è stato adottato da altri due importanti codici di condotta intervenuti nel settore di cui ci stiamo occupando, il codice di condotta neozelandese («*Farm Data Code of Practice*») e quello australiano («*Farm Data Code*»): v., con riguardo al codice neozelandese, L. Wiseman *et al.*, *Review of codes of conduct, voluntary guidelines and principles relevant for farm data sharing*, CTA Working Paper 19/01, December 2019, p. 12; J. Sanderson *et al.*, *What's behind the ag-data logo? An examination of voluntary agricultural data codes of practice*, in *International Journal of Rural Law and Policy*, 2018, p. 8.

[61] I *Privacy and Security Principles for Farm Data*, cit., asseriscono che tali principi «*are based upon the fundamental belief that farmers should own information originating from their farming operations*»; sulla stessa scia, nel Codice di condotta europeo si afferma

ISBN 978-88-495-5568-4

A riprova dell'importanza assegnata al modello proprietario nel contesto in esame, può notarsi come, anche nella consultazione lanciata dalla Commissione europea nell'ambito della strategia volta alla costruzione di un'economia comune dei dati, gli *stakeholders* del settore agricolo siano stati quelli che hanno maggiormente invocato il riconoscimento di un diritto di proprietà sui dati[62]. Ciononostante, è stato opportunamente rilevato come tale modello di regolazione, respinto a livello generale – seppur in modo ambiguo (cfr. art. 4, § 13, reg. UE n. 2023/2854) – dal legislatore europeo nel *Data Act*, presenti molte criticità anche nello specifico ambito dell'agricoltura digitale[63]. Infatti, se l'obiettivo è quello di tutelare maggiormente gli agricoltori, l'attribuzione ad essi di un diritto esclusivo sui c.d. dati agricoli può rivelarsi, da un lato, ultronea, rischiando di ostacolare in modo eccessivo la circolazione dei dati, e, d'altro lato, inefficace, potendo gli agricoltori comunque ritrovarsi ad accettare – in ragione di un'asimmetria di informazione o di potere negoziale – le condizioni contrattuali proposte dai fornitori di prodotti e servizi digitali operanti nell'ambito dell'agricoltura di precisione[64]. Invero, il diritto di proprietà è per natura cedibile ad altri soggetti, con la conseguenza che, in caso di alienazione, il dante causa perde definitivamente il controllo sui beni ceduti.

Alla luce di tali considerazioni, per venire incontro alle esigenze che si avvertono nel settore agricolo, sembra più proficuo un adattamento, e non uno stravolgimento, del modello regolatorio accolto nel *Data Act* (incentrato sulla logica dell'accesso invece che su quella proprietaria).

4. Come si è visto, il legislatore europeo riconosce che le peculiarità della filiera agricola possano giustificare un intervento regolatorio *ad hoc*, che affronti in modo specifico le questioni relative alla circolazione dei dati nell'ambito in esame. Tuttavia, non può negarsi che già il *Data Act* contiene

che «i diritti relativi ai dati prodotti nell'azienda agricola o durante le operazioni agricole sono attribuiti ("di proprietà di") all'agricoltore e possono essere ampiamente utilizzati da quest'ultimo». Sebbene dalle due iniziative auto-regolatorie emerga il medesimo paradigma ispiratore, non possono comunque trascurarsi le differenze che intercorrono tra i diversi concetti di "proprietà" conosciuti dagli ordinamenti giuridici in questione: per tutti, v. A. Gambaro, *Proprietà in diritto comparato*, in *Dig. disc. priv., Sez. civ.,* Torino, 1997, p. 502 ss.

[62] Commissione europea, *Annex to the Synopsis report. Detailed analysis of the public online consultation results on 'Building a European Data Economy'*, 19 settembre 2017, p. 24; posizione confermata anche dai rappresentanti delle imprese agricole intervenuti nell'Expert workshop sulla "*Common European Agricultural Data Space": M. Faraldi, How to build a Common European Agricultural Data Space. Workshop report*, 16 settembre 2020, p. 13.

[63] C. Atik, *Towards Comprehensive European Agricultural Data Governance*, cit., p. 710 ss.

[64] Id. *op. ult. cit*., p. 712 s.

 ISBN 978-88-495-5568-4

alcune misure di grande rilievo per gli agricoltori, utenti di prodotti connessi generatori di dati: su tutte, occorre richiamare la norma di cui all'art. 4, § 13, ove si prevede che il titolare dei dati non può utilizzare dati (non personali) del prodotto o del servizio correlato, che gli risultino prontamente disponibili, al fine di «ottenere informazioni sulla situazione economica, sulle risorse e sui metodi di produzione dell'utente, o sull'utilizzo da parte di quest'ultimo in qualsiasi altro modo che potrebbe compromettere la posizione commerciale sui mercati in cui l'utente è attivo». Sebbene tale disposizione non brilli per acribia linguistica, potendo sorgere qualche dubbio circa la qualificazione del divieto come norma imperativa che prevalga su qualsiasi previsione del contratto stipulato tra il titolare dei dati e l'utente[65], è evidente che la finalità sia quella di proteggere quest'ultimo da possibili usi distorti dei dati con conseguenze pregiudizievoli. E non può passare inosservato, per quanto interessa in questa sede, che tale previsione tenga conto proprio del contesto agricolo, come dimostra il considerando 27 del *Data Act*, ove si fa riferimento – come esempio di comportamento pregiudizievole – all'utilizzo, da parte del titolare dei dati, di informazioni agricole per «alimentare […] banche di dati sulle rese delle colture» e compiere previsioni sulle future stagioni di raccolta, con possibili ricadute negative per l'agricoltore-utente del prodotto connesso da cui le informazioni sono ricavate.

Se tale limitazione sugli usi secondari dei dati già soddisfa alcune esigenze di tutela degli utenti-agricoltori, non può ritenersi che ciò valga per l'intero reticolato normativo del *Data Act*. In particolare, è soprattutto l'ambito di applicazione che non risulta pienamente congeniale ai proble-

[65] Invero, l'art. 4, § 13, reg. 2023/2854 menziona nell'incipit la necessità di una previsione contrattuale che autorizzi il titolare dei dati ad utilizzare questi ultimi; in altri termini, l'utilizzo da parte del titolare presuppone il consenso dell'utente. In questo contesto, il legislatore introduce subito dopo il divieto riportato nel testo. Il dubbio sopra prospettato è dovuto, in particolare, alla circostanza che il titolare dei dati non può utilizzare questi ultimi, per ottenere le informazioni sopra indicate, «in qualsiasi altro modo che potrebbe compromettere la posizione commerciale sui mercati in cui l'utente è attivo», con il termine «altro» che potrebbe far pensare ad un'area di immunità garantita alle modalità di utilizzo previste dal contratto, sebbene tale immunità sia espressamente menzionata dall'art. 5, § 6 riferito ai destinatari dei dati e, dunque, *a contrario* potrebbe essere esclusa con riferimento agli utenti. D'altronde, se si sposa l'interpretazione più liberale, considerando lo squilibrio contrattuale tra il titolare dei dati e l'utente, si rischia di frustrare l'intento di proteggere quest'ultimo, così esautorando la stessa *ratio* della norma, senza considerare che è piuttosto difficile ipotizzare che un utente possa consapevolmente autorizzare un utilizzo dei dati che potrebbe compromettere la sua posizione commerciale sui mercati. Ad ogni modo, anche qualora si dovesse escludere la natura imperativa della norma in questione, l'eventuale clausola contrattuale pregiudizievole per l'utente non sarebbe comunque vincolante in quanto abusiva, a meno che il titolare dei dati non dimostri che vi sia stata un'effettiva negoziazione idonea a negare l'imposizione unilaterale (cfr. art. 13, reg. UE n. 2023/2854).

ISBN 978-88-495-5568-4

mi sottesi all'agricoltura di precisione. Il *Data Act*, infatti, da un lato, si applica soltanto ai «dati del prodotto», cioè dati generati dall'uso di un prodotto connesso[66] (art. 2, n. 15, reg. 2023/2854) e ai «dati di un servizio correlato»[67], cioè dati che rappresentano la digitalizzazione delle azioni o degli eventi degli utenti relativi al prodotto connesso, registrati intenzionalmente dall'utente o generati come sottoprodotto dell'azione dell'utente durante la fornitura di un servizio correlato da parte del fornitore (art. 2, n. 16, reg. 2023/2854); dall'altro lato, attribuisce diritti e tutele soltanto agli «utenti»[68] e, in parte, ai «destinatari dei dati»[69]. Di conseguenza, restano fuori dall'ambito applicativo i dati diversi da quelli sopra descritti e i soggetti diversi da quelli appena citati. In particolare, nonostante l'apprezzabile sforzo compiuto dal legislatore europeo nel tentativo di allargare la nozione di «prodotto connesso», correggendo la previsione inizialmente contenuta nella Proposta originaria[70], si dubita che possano rientrare nel campo di applicazione oggettivo i dati raccolti da una semplice videocamera che non sia parte di un prodotto connesso (come, ad es., una videocamera che non sia incorporata in un drone). In ambito agricolo, quindi, i dati sulla crescita delle colture o sul comportamento degli animali che potrebbero essere raccolti da una simile videocamera (non incorporata in un drone) e che potrebbero essere inseriti, anche manualmente, in banche dati da cui trarre, tramite successive elaborazioni, informazioni sulle imprese agricole "sorvegliate", non sarebbero sottoposti alle norme del *Data Act*[71]. Inoltre, sul piano soggettivo, quando l'utente di una macchina agricola intelligente non è un agricoltore, in quanto la macchina non è stata da quest'ultimo comprata o noleggiata, il *Data Act* non offre alcuna tutela all'agricoltore sui dati raccolti dalla macchina in questione nel terreno da lui coltivato.

Pertanto, nei casi in cui il *Data Act* non trova applicazione per limiti di carattere oggettivo e/o soggettivo, le imprese agricole potrebbero continuare ad essere vittime di quegli utilizzi di dati che l'art. 4, § 13 intende sopprimere.

Il *Data Act*, inoltre, nonostante dichiari di voler «garantire l'equità nella ripartizione del valore dei dati tra gli attori dell'economia [in questione]» (v. considerando 119), non contiene alcuna specifica disposizione che potrebbe favorire gli utenti nel ricevere direttamente un vantaggio economico in ragione dei ricavi ottenuti da altri soggetti operanti nella catena del va-

[66] Per la definizione di prodotto connesso, v. nota 33.

[67] Per la definizione di servizio correlato, v. nota 34.

[68] Per la definizione di utente, v. nota 35.

[69] Per la definizione di destinatario di dati, v. nota 36.

[70] C. Atik, *Horizontal intervention, sectoral challenges: Evaluating the data act's impact on agricultural data access puzzle in the emerging digital agriculture sector*, *in Computer Law & Security Review*, 2023, p. 7 s.

[71] Id., *op. ult. cit.*, p. 8.

 ISBN 978-88-495-5568-4

lore sprigionato dallo sfruttamento dei dati. Tale lacuna non è affatto irrilevante nel settore qui in esame, ove gli agricoltori sono ancora restii all'utilizzo di dispositivi tecnologici anche per la mancata partecipazione alla ripartizione dei ricavi generati dall'impiego altrui dei dati agricoli. Si pensi, ad esempio, ad un titolare dei dati che, grazie al contratto stipulato con l'utente-agricoltore, sia autorizzato a concedere a terzi (diversi dai destinatari indicati dall'utente) l'utilizzo dei dati, ottenendone notevoli guadagni (cfr. art. 4, § 14, reg. UE n. 2023/2854). A fronte, quindi, di possibili vantaggi economici unilaterali, per far sì che anche gli agricoltori abbiano un ritorno dal potere contrattualmente attribuito ai titolari dei dati, si potrebbe allora immaginare di rendere necessariamente a titolo oneroso il patto con cui l'utente acconsente di far arricchire il titolare dei dati in virtù di una futura commercializzazione degli stessi.

In conclusione, il futuro intervento regolatorio di stampo settoriale, che il considerando 27 del *Data Act* fa presagire, dovrebbe quindi – tra le possibili misure speciali – risolvere almeno le criticità sopra evidenziate, adottando, da un lato, una nozione di "dati agricoli" che prescinda dal tipo di strumento che li raccolga o generi e, dall'altro, assicurando tutela anche agli agricoltori che non risultino utenti dei prodotti connessi che raccolgono dati su elementi riferibili all'impresa agricola. In tal modo, estendendo il divieto già previsto dall'art. 4, § 13 del *Data Act* alle fattispecie finora escluse dal campo applicativo, si potrebbe senz'altro raggiungere una maggiore protezione per gli agricoltori. Inoltre, per favorire un'equa distribuzione del valore generato dai dati, la *lex specialis* potrebbe – come si è suggerito – escludere la natura gratuita del patto grazie al quale un'impresa tecnologica può ottenere da un agricoltore la facoltà di commercializzare i dati agricoli raccolti. Il *Data Act*, infatti, è silente sotto questo profilo, con la conseguenza che, allo stato attuale, il titolare dei dati potrebbe farsi concedere l'autorizzazione dall'utente senza fornirgli alcuna remunerazione.

In fondo, non c'è da stupirsi che le specifiche caratteristiche del settore in esame – noto per la strutturale debolezza in cui versano i produttori agricoli – richiedano l'adozione di una normativa *speciale*[72] anche in ordine all'accesso ai dati e alla loro condivisione: solo così può garantirsi il pieno sfruttamento delle nuove tecnologie, con un ritorno economico per tutti i soggetti della filiera agroalimentare, e non solo per alcuni.

[72] In generale, sul c.d. "eccezionalismo agricolo", v. per tutti A. Jannarelli, *Profili giuridici del sistema agro-alimentare e agro-industriale. Soggetti e concorrenza*, Bari, 2018, p. 13 ss.

ISBN 978-88-495-5568-4

Mariangela Ziccardi

Digitalizzazione e innovazione tecnologica nei contratti di filiera agroalimentare

Sommario: 1. L'incidenza delle nuove tecnologie sulle dinamiche dell'economia moderna. – 2. L'innovazione nella filiera agroalimentare quale strumento per la realizzazione di un nuovo paradigma produttivo. Difformità strutturali e funzionali tra il modello della filiera corta e quello dell'agricoltura industrializzata. – 3. Le possibili misure tecnologiche per favorire il connubio innovazione-sostenibilità delle grandi imprese del settore agroalimentare: dispositivi IoT (*Internet of things*), *blockchain* e *smart contracts*. – 4. Principali profili di criticità derivanti dall'impiego della tecnologia nel comparto agricolo: rilievi conclusivi.

1. L'inarrestabile processo di digitalizzazione e l'intensità dell'avanzamento tecnologico hanno generato, nel tempo, una completa trasformazione della fisionomia della realtà, conquistata e dominata dai prodigi offerti dalle frontiere della tecnologia[1].

Gli strumenti digitali e le loro molteplici applicazioni sono diventati essenziali per lo sviluppo socio-economico e culturale della collettività[2], tant'è che ormai ogni genere di attività – da quelle prettamente connesse alla sfera intima della persona a quelle economiche e produttive latamente intese[3] – viene compiuta avvalendosi di sistemi tecnologici sempre piú so-

[1] Sulle potenzialità degli strumenti tecnologici che consentono di creare una società fortemente avanzata (la c.d. «società tecnologica»), tanto che ormai essa «si costruisce e si esprime» mediante la tecnologia, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, III, *Situazioni soggettive*, 4ª ed., Napoli, 2020, p. 130 ss.; ma già Id., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, 2005, p. 78; C. Perlingieri, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici*, in *Rass. dir. civ*., 2015, p. 1235 ss. e A. Alpini, *La trasformazione digitale nella formazione del civilista*, in *Tecn. dir*., 2021, p. 6.

[2] R. Tommasini, *Introduzione*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Atti del 14° Convegno Nazionale, Napoli, 2020, p. 90; A. Alpini, *L'impatto delle nuove tecnologie sul diritto*, in *comparazionedirittocivile.it*, dicembre 2018, p. 60 ss.; S. Rodotà, *Il diritto di avere diritti*, Bari, 2012, p. 318, secondo il quale l'uomo è sommerso in una fitta rete di sistemi informatici e robotici «che consente di estendere la [sua] capacità di comunicare e agire; si modifica lo spazio della presenza dell'umano» e anche S. Giova, *La persona nel contesto digitale: considerazioni conclusive*, in *Tecn. dir*., 2023, p. 326 ss.

[3] Sull'impatto dell'innovazione tecnologica nel sistema ordinamentale, con riferimento al mutamento delle modalità di svolgimento dei rapporti e dell'attività economica, P. Perlingieri, Privacy *digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap*.,

 ISBN 978-88-495-5568-4

fisticati[4]; in questa direzione, tanto nei rapporti personali quanto in quelli patrimoniali si assiste inesorabilmente al progressivo indebolimento della presenza dell'uomo il quale, richiamato dall'affascinante suono dell'apparato tecnologico, ne risulta talvolta completamente travolto[5], sí da mettere in discussione il suo ruolo e la sua percezione di sé[6].

In altri termini la tecnologia, nata originariamente come ausilio vòlto a migliorare le capacità dell'uomo, diviene nel tempo uno strumento che tende a sostituirsi all'intelligenza umana[7], capace di semplificare e/o dematerializzare ogni tipo di attività e, persino, di interagire con l'uomo[8].

2018, p. 481 ss.; D. Di Sabato, *Diritto e* new economy, Napoli, 2020, spec. p. 15 ss. e, di recente, si v. I. Martone, *Gli* smart contracts*. Fenomenologia e funzioni*, Napoli, 2022, p. 13 ss., la quale rileva che nell'attuale società contrassegnata dalla digitalizzazione «le decisione [per l'uomo] di avvalersi dello strumentario tecnologico finisce per rivelarsi scelta necessaria a fronte della incontrollata velocità con la quale il processo di evoluzione avanza».

[4] P. Perlingieri, *Note sul «potenziamento cognitivo»,* in *Tecn. dir*., 2021, p. 209, il quale sottolinea che «[la] società [è] caratterizzata sempre piú da una commistione di esperienze fisiche e virtuali, dove l'*online* e l'*offline* contribuiscono a comporre la "complessiva realtà" e dove ormai le informazioni anche sensibili circolano in rete», compromettendo inevitabilmente anche la tradizionale concezione della *privacy*; Id., *Relazione conclusiva*, in Id., S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 379 ss.; F. Di Ciommo, *Archivi digitali (onnivori) e diritti fondamentali recessivi*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 246, il quale fa notare che «la rete Internet cresce, e insieme ad essa le infinite altre reti di interconnessione, nuovi algoritmi si affermano […] e, in definitiva, il mondo che noi abitiamo cambia radicalmente e ad una velocità mai considerata prima» e A. Alpini, *Identità, creatività e condizione umana nell'era digitale,* in *Tecn. dir*., 2020, p. 4 ss., secondo la quale le nuove tecnologie hanno ridotto l'identità umana a «materia prima del processo tecnologico. L'individuo, incluso nell'apparato tecnologico, finisce per essere un dato operazionale della macchina».

[5] L'uomo appare cosí «logorato e […] irriconoscibile dal progredire di scienza e tecnologie», S. Rodotà, *Tecnopolitica*, Bari, 1996, p. 136 e A. Federico, *Il* nomos *della 'infosfera',* in *Rass. dir. civ.,* 2022, p. 533 ss. e spec. p. 537, rileva che «l'infosfera è diventata l'ambiente reale nel quale si svolge l'esistenza, perché il mondo è stato progressivamente adattato, in un modo invisibile e sovente inconsapevole, alle tecnologie digitali costruendo un peculiare involucro nel quale le interazioni umano-computer sono diventate di nuovo somatiche […]. Ogni giorno il mondo è modificato e ri-ontologizzato per essere conformato alle capacità dei sistemi di AI».

[6] F. Anelli, *Introduzione*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 305 ss., mette in evidenza che nella nostra epoca si registra un cambiamento di prospettiva, e cioè «[la] tradizionale domanda su come io debba usare la tecnologia [muta in] come la tecnologia stia utilizzando me e, prometta o minacci di utilizzarmi nel prossimo futuro», ricordando le riflessioni di L. Floridi, *La quarta rivoluzione. Come l'infosfera sta cambiando il mondo*, Milano, 2017.

[7] A tal proposito fa notare P. Perlingieri, *Note sul «potenziamento cognitivo»*, cit., p. 209, che «occorre sia allontanare il convincimento che i computer fanno solo quello che sono programmati a fare […], sia accettare che essi, per velocità, precisione e memoria, già allo stato […] sono superiori agli esseri umani, quali strumenti di incredibile utilità»; v. anche E. Caterini, Artificial Intelligence, *persona e soggetto,* in *Tecn. dir*., 2022, p. 207 ss.

ISBN 978-88-495-5568-4

Tra l'altro, la portata del fenomeno può essere saggiata mediante l'analisi dell'evoluzione della contrattazione a partire dall'utilizzo delle nuove tecnologie in àmbito negoziale: in particolare, mentre inizialmente nel contratto telematico l'utilizzo del computer rappresenta un mero *medium* di comunicazione funzionale a trasmettere la proposta e ricevere l'accettazione dell'accordo perfezionato tra le parti[9], successivamente già nel contratto cibernetico, quale peculiare figura del contratto telematico, il contenuto del regolamento negoziale, seppur entro alcuni limiti e nel rispetto delle istruzioni del *software*, viene affidato alle determinazioni del computer[10]; per poi giungere infine alla fase attuale, quella degli *smart contracts* (i contratti c.dd. intelligenti)[11] ove l'apporto umano all'intero ciclo negoziale è grandemente ridotto[12]. Negli anni si è dunque assistito ad una graduale

[8] La pervasività della tecnologia ha generato «l'emersione di una varietà di surrogati artificiali della persona ovvero delle relative volizioni mediante entità non naturali […] modellate sull'individualità umana», cosí C. Perlingieri, *L'incidenza dell'utilizzazione della tecnologia robotica nei rapporti civilistici,* cit., p. 1236. Sull'interazione uomo-macchina si v. le riflessioni di P. Femia, *Essere norma. Tesi sulla giuridicità del pensiero macchinico*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 65 ss., il quale osserva che «l'interazione tra intelligenza artificiale e intelligenza umana provoca un'ibridazione intellettiva, nella quale nessuna delle due riesce a distinguere se stessa finché opera e non riflette […]. È impossibile separare l'azione dell'uno e dell'altro, poiché ciascuno apprende come comportarsi dal comportamento dell'altro ed i risultati non sono prevedibili. Al contrario […], quando la macchina riflette, essa opera come entità separata dall'uomo. E in quel momento l'uomo non ha accesso ai pensieri della macchina: l'uomo traduce le decisioni autonome della macchina, non i suoi funzionamenti interni»; e v. anche G. Teubner, *Personalità giuridica digitale? Sullo* status *privatistico degli agenti* software *autonomi, ivi*, p. 99 ss.

[9] Sulla contrattazione per via telematica si rinvia in particolare a P. Perlingieri, *Metodo categorie e sistema nel diritto del commercio elettronico*, in Id., *Il diritto dei contratti fra persona e mercato. Problemi del diritto civile*, Napoli, 2003, p. 652 ss.; G. Perlingieri, *Appunti sul contratto telematico*, Napoli, 2000, p. 1 ss.; C. Perlingieri, *Il contratto telematico*, in A. Di Amato (a cura di), *Appunti di diritto dei mezzi di comunicazione*, Napoli, 2006, p. 239; S. Giova, *La conclusione del contratto via Internet*, Napoli, 2000, p. 7 ss.; Ead., *Le vendite* online, in C. Perlingieri e L. Ruggeri (a cura di), *Internet e diritto civile*, Napoli, 2015, pp. 149-163 e F. Delfini, *Il commercio elettronico*, in *Tratt. dir. econ.*, diretto da E. Gabrielli ed E. Picozza, Padova, 2004.

[10] Sul contratto cibernetico si v. G. Finocchiaro, *La conclusione del contratto telematico mediante i «*software agents*»: un falso problema giuridico?, Brevi considerazioni*, in *Contr. impr*., 2002, p. 500 ss.; G. Sartor, *Gli agenti* software*: nuovi soggetti del ciberdiritto?, ivi,* 2022, p. 465 ss.; F. Bravo, *Contrattazione telematica e contrattazione cibernetica*, Milano, 2007 e R. Borruso, S. Russo e C. Tiberi, *L'informatica per il giurista. Dal* bit *a Internet*, Milano, 2009.

[11] Diversamente I. Martone, *Gli* smart contracts, cit., p. 53, fa notare che «la traduzione "contratto intelligente", per quanto già largamente diffusa nella prassi, al pari di altre etichette comunemente impiegate […], oltre a sollevare svariate perplessità, si rivela meramente descrittiva».

[12] Con riferimento all'incidenza delle nuove tecnologie sull'evoluzione delle modalità

 ISBN 978-88-495-5568-4

spersonalizzazione del contratto: le potenzialità della tecnologia ne hanno determinato la sua «disumanizzazione»[13]: «la tecnica si fa contratto», la macchina tenta di sostituire i contrenti, essa «non è piú un mero tramite, perché è il contratto»[14].

La tecnologia travolge l'intero panorama conoscitivo: il suo impiego appassiona sempre piú settori: si pensi a quello finanziario[15], sanitario[16], automobilistico e, non da ultimo a quello agroalimentare[17].

Con riferimento al settore dell'*agrifood*, le imprese italiane mostrano

della contrattazione, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti,* IV, *Attività e responsabilità*, 4ª ed., Napoli, 2020, p. 85 ss.; specificamente sugli *smart contracts*, si segnalano, D. Di Sabato, *Gli* smart contracts*:* robot *che gestiscono il rischio contrattuale,* in *Contr. impr.,* 2017, p. 378 ss.; G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim*., 2018, p. 441 ss.; M. Maugeri, *Autonomia e costruzione dello spazio digitale*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 151 ss.; L. Di Nella, Smart Contract*,* Blockchain *e interpretazione dei contratti*, in *Rass. dir. civ*., 2022, p. 933 ss.; I. Martone, *o.c.*, *passim*; M. Giaccaglia, *Questioni (ir)risolte in tema di* smart contract*. Per un ritorno al passato*, in *Tecn. dir*., 2022, p. 333 ss. ed E. Maio, *La gestione dell'inadempimento contrattuale negli* smart contract, in *Actualidad jur. iberoam*., 16, 2022, pp. 1334-1347.

[13] Si tratta della nota espressione utilizzata da G. Oppo, *Disumanizzazione del contratto*?, in *Riv. dir. civ*., 1998, p. 525 ss., in risposta a N. Irti, *Scambi senza accordo*, in *Riv. trim*., 1998, I, p. 347 ss., il quale replica con *È vero ma… (Replica a Giorgio Oppo)*, *ivi*, 1999, I, p. 273.

[14] A.M. Benedetti, *Contratto, algoritmi e diritto civile transnazionale: cinque questioni e due scenari,* in *Riv. dir. civ*., 2021, p. 411 ss., il quale rileva che la nuova frontiera del diritto «è oltre: [programmi-macchine] che prendono il posto dei contraenti-umani [gestendo] la formazione, l'esecuzione, le sopravvenienze: un "supercontratto»; ma già P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, IV, cit., spec. pp. 79 e 85 s., secondo il quale «le forti trasformazioni sociali, l'internazionalizzazione dell'economia, le innovazioni tecnologiche hanno avuto sulla nozione di contratto un impatto dirompente» e Id., *Il diritto dei contratti fra persona e mercato*, cit.

[15] Sul tema R. Lener, *Tecnologie e attività finanziaria*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., p. 197 ss., il quale osserva che «l'area dei servizi finanziari si è invero dimostrata particolarmente fertile per le nuovissime tecnologie; sono infatti pochi i servizi che non si sono "evoluti" in senso tecnologico; anche quelli in cui l'attività intellettuale umana e il contatto personale erano tradizionalmente ritenuti essenziali hanno subíto fortissimi cambiamenti». Si pensi ai c.dd. *robo-advisor* ("consulenti *robot*"), o alle piattaforme che agevolano l'incontro di imprese e finanziatori, dando origine alle varie *crowdfunding* o, infine, al c.d. *trading* algoritmico (*High Frequency Trading*) con il quale un algoritmo, mediante l'acquisizione e la combinazione dei dati, esegue gli investimenti finanziari.

[16] In argomento si v. V. Rotondo, *Responsabilità medica e autodeterminazione della persona*, Napoli, 2020, spec. p. 159 ss., il quale fa notare che «le tecnologie impiegate in sanità, [*i.e.*, la robotica] in un prossimo futuro, si candidano a fornire in autonomia prestazioni affidate oggi esclusivamente ad un agere umano».

[17] Sull'impatto della tecnologia nei vari settori, Aa.Vv., *Diritto, robotica e nuove frontiere tecnologiche*, in *Dir. merc. ass. fin*., Napoli, 2018.

ISBN 978-88-495-5568-4

particolare attrazione verso l'utilizzo delle soluzioni offerte dalla tecnologia nell'ottica di aumentare la produttività e la competitività sul mercato e, al contempo, favorire un'agricoltura sostenibile[18] finalizzata cioè ad appagare i bisogni delle generazioni presenti senza pregiudicare quelli delle generazioni future, in coerenza, del resto, con gli obiettivi dell'Agenda 2030 delle Nazioni Unite per lo sviluppo sostenibile[19].

Purtuttavia se è innegabile che il ricorso agli strumenti tecnologici nell'*agrifood* e in generale nei vari settori appare essenziale per far fronte alle nuove esigenze promananti dal tessuto socio-economico, occorre far notare che al progresso tecnologico non corrisponde la medesima rapidità di intervento sotto il profilo normativo-regolamentare[20].

In altri termini, dinanzi a cambiamenti cosí repentini innescati dalla digitalizzazione il legislatore – coadiuvato dalla laboriosa opera della dottrina e della giurisprudenza – in parte tenta di «insegu[ire], in parte [cerca di] indirizza[re] il cambiamento»[21], dovendo inevitabilmente fare i conti con nuovi interrogativi ai quali affannosamente tenta di dare risposte[22].

[18] Il concetto di sostenibilità agroalimentare poggia su tre pilastri fondamentali: quello ambientale, quello economico e quello sociale, secondo l'approccio multidimensionale elaborato dalla FAO (1991). L'Organizzazione delle Nazioni Unite per l'alimentazione e l'agricoltura, infatti, ritiene che sono indicatori di sostenibilità agricola: «la gestione e la conservazione della base delle risorse naturali e l'orientamento del cambiamento tecnologico e istituzionale in modo tale da garantire il raggiungimento e la continua soddisfazione dei bisogni umani per le generazioni presenti e future. Tale sviluppo conserva la terra, l'acqua, le risorse genetiche, non è degradante dal punto di vista ambientale, è tecnicamente appropriato, economicamente sostenibile e socialmente accettabile». Si v. altresí la riforma costituzionale degli artt. 9 e 41 cost. (l. cost. 11 febbraio 2022 n. 1) con la quale l'ambiente diviene oggetto di specifica tutela da preservare anche nell'interesse delle generazioni future, allontanandosi cosí da una visione incentrata sull'uomo per andare verso una prospettiva biocentrica.

[19] L'Agenda, costituita da 17 obiettivi per lo sviluppo sostenibile (*Sustainable Development Goals*), è stata sottoscritta nel 2015 da 193 Paesi membri delle Nazioni Unite e approvata dall'Assemblea Generale dell'ONU. I 17 *goals* impongono l'adozione da parte dei governi di strategie di sviluppo sostenibile, equilibrato e inclusivo, considerata la profonda correlazione tra dinamiche economiche, crescita sociale e qualità ambientale. Con riferimento al settore dell'agrifood si v. in particolare l'obiettivo n. 2: «Azzerare la fame, realizzare la sicurezza alimentare, migliorare la nutrizione e promuovere l'agricoltura sostenibile»; il n. 9: «Promuovere l'industrializzazione sostenibile e inclusiva e favorire l'innovazione» e il n. 12: «Garantire modelli di consumo e produzione sostenibili».

[20] P. Perlingieri, *Relazione conclusiva*, cit., p. 383, il quale fa notare che «cresce la consapevolezza di una sorta di impotenza a regolare un fenomeno cosí tecnologicamente complesso e globale» e, concordemente, R. Tommasini, *Introduzione*, cit., p. 92, il quale osserva che «aggiornare tutto con continuità nei diversi settori è impossibile, mentre le tecnologie digitali possono farlo in tempo estremamente ridotto, se non addirittura contestualmente».

[21] I. Martone, *Sulla trasmissione a causa di morte del «patrimonio digitale»*, in *Tecn. dir.,* 2020, p. 423.

[22] «Si discorre a tal proposito di diritto delle nuove tecnologie: un diritto sempre piú specializzato e la specializzazione implica una conoscenza approfondita del contesto eco-

 ISBN 978-88-495-5568-4

2. Nella filiera agroalimentare – intendendo come tale il percorso che l'alimento segue dalla produzione fino al consumatore finale – l'innovazione coinvolge i vari attori della catena e sarebbe teleologicamente orientata al soddisfacimento dei loro diversi interessi.

In effetti, nell'ottica imprenditoriale, il binomio impresa-innovazione rappresenterebbe quel *quid melius* che garantirebbe non soltanto maggiore produttività, competitività, sostenibilità, nonché contenimento dei costi, ma favorirebbe anche la tracciabilità del prodotto nella catena di approvvigionamento alimentare (c.d. *supply chain agrifood*); per coloro che invece sono parte attiva del ciclo produttivo, l'innovazione migliorerebbe l'efficienza e la qualità del lavoro essendo rivolta, principalmente, alla meccanizzazione dei processi produttivi e alla digitalizzazione delle procedure di monitoraggio della filiera; infine, l'innovazione avrebbe evidenti ricadute sul consumatore in termini di trasparenza sulla provenienza e sui processi di lavorazione dei prodotti e, quindi, consentirebbe una maggiore tracciabilità e sicurezza alimentare nella duplice accezione di *food safety* e *food security*[23].

Invero, nell'ontologica disparità di forze esistente nella contrattazione tra imprenditore (professionista) e consumatore – tale di fatto da giustificare tutti gli interventi normativi per mitigare le asimmetrie informative tra i contrenti – l'innovazione nel comparto produttivo agricolo assicurerebbe al consumatore un'informazione adeguata per quantità e qualità e, di conseguenza, tanto piú elevato è il livello di consapevolezza raggiunto, tanto maggiore è il tasso di efficienza e di competitività del mercato[24].

In sostanza, dunque, le soluzioni tecnologiche nel settore agricolo realizzerebbero quella cooperazione e interazione tra gli operatori della filiera funzionali, in ultima istanza, all'adozione da parte del consumatore di scelte alimentari consapevoli, riducendo il rischio di frodi e contraffazioni (c.d.

nomico e sociale: specializziamo per ricondurre a sistema una nuova regola, tant'è che in questa fase del processo di innovazione tecnologica siamo dinanzi ad un vero e proprio "cantiere normativo"», P. Femia, *Intelligenza artificiale nell'esperienza della legalità costituzionale*, relazione tenuta al Convegno su: *Nuove tecnologie e cultura del diritto civile in occasione della presentazione della Rivista scientifica Tecnologie e Diritto*, Dipartimento di Giurisprudenza, Università degli Studi di Napoli Federico II, 24 e 25 novembre 2022.

[23] Ove per *food safety* si intendono gli aspetti legati alla sicurezza quali l'igiene e la salubrità dell'alimento, invece con l'espressione *food security* ci si riferisce al diritto di accesso ad una quantità di cibo sufficiente per condurre una vita dignitosa, secondo un'accezione economico-sociale.

[24] P. Perlingieri, *L'informazione come bene giuridico*, in Id., *Il diritto dei contratti fra persona e mercato*, cit., p. 336 s., il quale osserva che «conoscere è potere, l'informare e l'essere informati rappresentano una necessità dell'intero sistema»; altresí, L. Rossi Carleo, *Il diritto all'informazione: dalla conoscibilità al documento informativo*, in *Riv. dir. priv.,* 2004, p. 349 ss. e A. Gentili, *Informazione contrattuale e regole dello scambio, ivi*, p. 558 ss.

ISBN 978-88-495-5568-4

fenomeno dell'*Italian sounding*)[25] che minerebbero non soltanto la salute del consumatore ma anche l'efficienza dello stesso mercato[26].

Nella direzione tracciata, appare ragionevole ritenere che il ricorso allo strumentario tecnologico nel comparto agricolo sembrerebbe rivelarsi, allo stato attuale, poco confacente alla c.d. filiera corta o a Km zero[27] poiché, a ben vedere, essa mira a stabilire una relazione diretta tra il produttore e il consumatore, eliminando o quantomeno riducendo grandemente le figure professionali coinvolte dalla produzione iniziale alla distribuzione.

Tale peculiarità della filiera corta permette di abbattere l'inquinamento e gli sprechi, di ottimizzare l'ecosostenibilità e di valorizzare la qualità del prodotto proprio in forza del rapporto di fiducia e di solidarietà tra produttore e consumatore che consente a quest'ultimo di accedere direttamente a tutte le informazioni che riguardano la tracciabilità del prodotto[28].

Per di piú, l'impiego della tecnologia comporta di per sé un aggravio di costi i quali, se sopportati dall'impresa della filiera corta, inevitabilmente

[25] Il fenomeno si riferisce all'utilizzo di denominazioni, immagini, combinazioni di marchi ecc… che evocano il *Made in Italy* su prodotti agroalimentari che italiani non sono. Secondo un'indagine della Coldiretti, nel mondo il valore dell'*Italian sounding* agroalimentare è salito a 120 miliardi di euro nel 2022, il che significa che il 73% degli italiani in viaggio all'estero si è imbattuto almeno una volta in una specialità *Made in Italy* contraffatta.

[26] P. Perlingieri, *La persona e i suoi diritti*, cit., p. 97 s., fa notare che «lo sviluppo non si riduce alla semplice crescita economica, ma deve comportare la promozione dell'uomo […]. La società tecnologica resti societas solidale e, attenta ai contenuti, ai valori, alla cultura della dignità umana […]. Il sistema economico ed il processo di produzione traggono vantaggio quando i valori personali sono pienamente rispettati»; Id., *Mercato, solidarietà e diritti umani*, in Id., *Il diritto dei contratti tra persona e mercato*, cit.

[27] I modelli principali della filiera corta sono i c.dd. *farmers' market* (mercati degli agricoltori), i GAS (gruppi di acquisto solidale), le vendite in cassetta (*box scheme*) e la *community-supported agricolture* (CSA), tutti accomunati dalla volontà di promuovere la sostenibilità, la biodiversità, la tradizione culturale e la solidarietà. Già nella PAC (Politica Agricola Comune) 2014-2020, la filiera corta viene considerata uno strumento per facilitare il raggiungimento degli obiettivi europei in materia di sviluppo rurale e, da ultimo, il legislatore italiano è intervenuto con la l. 17 maggio 2022, n. 61 (*Norme per la valorizzazione e la promozione dei prodotti agricoli e alimentari a chilometro zero e di quelli provenienti da filiera corta*) con la quale vengono introdotte alcune disposizioni volte a favorire la commercializzazione e il consumo dei prodotti provenienti dalla filiera corta, sul solco delle raccomandazioni del Parlamento europeo che promuove la strategia *Farm to Fork* 2020 ("dal produttore al consumatore") per conseguire gli obiettivi del *Green Deal* europeo (2019), il cui scopo principale è quello di raggiungere la neutralità climatica entro il 2050. In argomento si v. M.A. Ciocia, *L'iniziativa economica privata nella transizione ecologica. Primi spunti ricostruttivi*, in *Riv. giur. Mol. Sannio*, 2022, p. 89 ss.

[28] G. Guzzardi, *Formalismo negoziale e tutele nei contratti della filiera agroalimentare*, in *Contratti*, 2022, p. 551 ss., fa notare che «la crescente sensibilità dei consumatori nei confronti della c.d. "agricoltura sostenibile", perché piú attenta a tematiche quali il rispetto dell'ambiente, il risparmio energetico, la tutela della biodiversità, l'origine dei prodotti, la sicurezza alimentare e della forza lavoro impiegata, [favorisce] la c.d. "filiera corta", a tutto vantaggio di produttori e piccoli dettaglianti».

 ISBN 978-88-495-5568-4

ricadrebbero sul consumatore, sí da vanificare di fatto l'obiettivo stesso di tale sistema produttivo che è quello di ridurre i costi del prodotto finale grazie all'eliminazione ovvero alla riduzione dei vari soggetti intermediari.

Viceversa, sembrerebbe che la tecnologia ben si armonizzerebbe con la c.d. filiera lunga la quale prevede un elevato numero di soggetti (grossisti, distributori, negozi al dettaglio) nonché di passaggi dalla produzione al consumo finale.

Si tratta del modello della grande distribuzione organizzata (GDO) o dell'agricoltura industrializzata – contrapposto al precedente della filiera corta o della c.d. agroecologia[29] – tipico dei prodotti che necessitano di numerose trasformazioni; in questi casi, l'impiego della tecnologia consentirebbe di aumentare la produzione e, contestualmente, di ridurre i costi.

E, invero, anche le recenti misure economiche per sostenere l'innovazione nel settore dell'*agrifood* sono destinate prevalentemente alle grandi realtà imprenditoriali trattandosi per lo piú di incentivi rivolti alle imprese dedite alla trasformazione di prodotti agricoli, il che dà prova della fisiologica estromissione delle imprese della filiera corta dai finanziamenti agevolati.

3. Un'ulteriore conferma che l'innovazione nel settore agricolo risulta calibrata sul modello della grande distribuzione organizzata (GDO) è rappresentata dal fatto che l'Italia nell'anno 2022 ha registrato una crescita dell'*export* agroalimentare nel suo complesso pari al 15,3% rispetto al 2021, sí da rendere il nostro il secondo Paese dell'Unione europea per incidenza dell'*agrifood* sul PIL (circa il 4%)[30]. A ben vedere, tale dato non è di poco momento in quanto conferma che le soluzioni offerte dalla tecnologia possono trovare applicazione soltanto con riferimento a quei prodotti alimentari non soggetti ad obsolescenza nel breve e medio termine quali sono quelli destinati all'*export*, con esclusione quindi dei prodotti agricoli facilmente deteriorabili caratteristici della filiera corta.

[29] Quello dell'agroecologia è il modello produttivo che nasce dai produttori ed è congeniale alla realizzazione della c.d. sovranità alimentare *i.e.*, democrazia alimentare, intesa quale «diritto dei popoli a del cibo sano e culturalmente appropriato prodotto con metodi ecologicamente sani e sostenibili, [nonché] il loro diritto di definire i propri sistemi agroalimentari» (Dichiarazione di Nyeleni, 2007; concetto ribadito dall'art. 15 della Dichiarazione ONU sui diritti dei contadini del 2018, nonché dalla PAC 2023-2027). A partire dal 2020 diversi Paesi hanno inserito la sovranità alimentare nelle loro Costituzioni e legislazioni, mentre in Europa soltanto il Canton Ticino. Sul tema si v. L. Paoloni, *La sostenibilità "etica" della filiera agroalimentare*, in *Riv. dir. alim.*, 4, ottobre-dicembre 2020, consultabile su *rivistadirittoalimentare.it*, la quale osserva che le piccole imprese hanno un ruolo fondamentale per garantire la sovranità alimentare anche se dal 7° censimento generale dell'agricoltura dell'ISTAT (periodo 7 gennaio-30 luglio 2021 e diffuso il 23 settembre 2022) risulta che in Italia, negli ultimi anni, sono scomparse 1/3 delle piccole aziende agricole e, che, invece, sono aumentate quelle di grandi dimensioni.

[30] V. report del CREA (Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria), su *crea.gov.it.*

ISBN 978-88-495-5568-4

D'altronde, il modello organizzativo e produttivo della c.d. agricoltura 4.0 (*smart agrifood*) è il risultato dell'applicazione di un insieme di tecnologie in campo alimentare che consentono di realizzare un'agricoltura di precisione (*precision farming*) finalizzata ad agevolare le grandi imprese nello svolgimento della propria attività generando un circolo virtuoso a cascata in grado cioè di creare valore non soltanto per la singola azienda ma anche per tutti i *partners* della filiera produttiva[31].

E invero, l'intento di favorire il connubio innovazione-sostenibilità emerge fin dall'art. 3 del Trattato sull'Unione europea (Maastricht 1993) il quale pone, tra gli obiettivi, lo sviluppo sostenibile, basato su una crescita economica equilibrata, su un'economia sociale di mercato fortemente competitiva che tenda alla piena occupazione e al progresso sociale, al miglioramento della qualità dell'ambiente, al progresso scientifico e tecnologico, sí da realizzare la solidarietà tra le generazioni e tra gli stessi Stati membri, la coesione economica, sociale e territoriale.

Da allora numerose sono state negli anni le iniziative finalizzate ad incentivare l'innovazione nel settore dell'*agrifood* e, tra le piú recenti, si ricorda in particolare il Documento approvato dalla Commissione europea (gennaio 2021), denominato *List of potential agricultural practices that eco-schemes could support*, in cui si individuano – definendo i contenuti della nuova PAC (politica agricola comune del Consiglio europeo 2023-2027)[32] – una serie di pratiche dell'agricoltura digitale in grado di migliorare le prestazioni economiche, sociali, ambientali e climatiche per una gestione piú efficiente delle risorse in termini di sostenibilità; o ancóra ai fondi del Piano Nazionale Ripresa e Resilienza (PNRR 2021) connessi alla strategia europea della digitalizzazione e innovazione del sistema produttivo per avviare la c.d. rivoluzione *green*.

E dunque, seguendo il percorso tracciato, occorre sondare quali siano in concreto le soluzioni innovative che le grandi imprese del settore agricolo possono adottare per rispondere alle nuove sfide promananti dal mercato.

In un primo gruppo possono essere ricomprese quelle misure tecnologiche di natura applicativa funzionali alla realizzazione di un'agricoltura

[31] Secondo i risultati di una ricerca realizzata dall'Osservatorio *Smart Agrifood* della *School of Management* del Politecnico di Milano e del Laboratorio RISE (*Research & Innovation for Smart Enterprises*) dell'Università degli Studi di Brescia, presentata in occasione del Convegno: *Da adozione a valorizzazione: la sfida dello* Smart agrifood (16 marzo 2023), in Italia nel 2022 il mercato dell'agricoltura 4.0 è ulteriormente cresciuto (oltre 2 miliardi di euro), registrando una crescita del +31% rispetto al 2021.

[32] I tre regolamenti che compongono il pacchetto di riforma della PAC (2023-2027) firmati dal Consiglio e dal Parlamento europeo il 6 dicembre 2021 prevedono l'introduzione di piani strategici a livello degli Stati membri che consentono ai governi nazionali di adattare le disposizioni della PAC ai bisogni delle loro comunità agricole in collaborazione con le autorità locali e le parti interessate.

 ISBN 978-88-495-5568-4

digitale quali i droni e i sistemi di telerilevamento (o rilevazione satellitare): tecnologie con finalità diagnostica-investigativa che mirano a raccogliere a distanza informazioni per controllare e valutare lo stato di salute sia del suolo che delle colture; strumenti strategicamente idonei a supportare le scelte gestionali delle aziende agricole e a permettere l'analisi delle variabilità presenti in un campo.

Si tratta dei dispositivi IoT (*Internet of things*) che consentono di ottenere dati fondamentali per valutare in tempo reale diversi parametri di natura ambientale, climatica e colturale; tali strumenti forniscono agli agricoltori informazioni, come quelle sui mutamenti climatici, di notevole rilevanza nell'àmbito dei processi produttivi, permettendo una puntuale individuazione degli obiettivi produttivi da raggiungere sia quantitativi che qualitativi[33].

In tale gruppo vanno altresí ricomprese le macchine agricole integrate da tecnologie fortemente avanzate (es. i sistemi di telemetria o i *monitor touchscreen*) e anche i sistemi di guida automatizzata che fornirebbero all'uomo un apporto considerevole nella coltivazione.

Ma lo scenario aperto dalle frontiere della tecnologia si spinge oltre lanciando ulteriori opportunità e nuove sfide anche per il settore agroalimentare: il riferimento è all'utilizzo della tecnologia *blockchain* quale meccanismo di *database* avanzato che consente la condivisione trasparente di informazioni (c.dd. registri distribuiti), nonché dello *smart contract*[34] la cui essenza risiede nell'autogestione programmata del rapporto contrattuale, riducendo fortemente l'intervento umano.

In particolare quest'ultimo, che costituisce un'applicazione evolutiva della *blockchain*[35] – di là dalle numerose e incerte elaborazioni dottrinali[36] –

[33] C. Faleri, *Transizione ecologica e sostenibilità sociale per un'Agricoltura 4.0*, in *Lav. dir.*, 2022, p. 449 ss. e v. anche G. Remotti, *Possibili funzioni ausiliarie delle tecnologie blockchain per marchi e indicazioni di origine: tracciabilità della filiera agroalimentare, dinamica competitiva e meccanica mercantile*, in *MediaLaws, Riv. dir. media*, 3, 2021, p. 29 ss.

[34] Locuzione utilizzata per la prima volta da N. Szabo, *The idea of* Smart Contracts, 1997, su *https://tinyurl.com/y43w33l2*.

[35] Fermo restando che il raggio di operatività di tali figure va ben oltre il sistema dei registri distribuiti (in questo senso, cfr. I. Martone, *Gli* smart contracts, cit., p. 52 e M. Giaccaglia, *Gli* Smart Contracts*. Vecchi e nuovi (?) paradigmi contrattuali nella prospettiva della protezione dei consumatori,* in *Dir. merc. tecn*., 2020, p. 120 s. *Contra*, F. Di Ciommo, *Smart contract e (non-) diritto. Il caso dei mercati finanziari,* in *Nuovo dir*., 2019, p. 270, secondo il quale non sarebbe opportuno ritenere che gli *smart contracts* siano «figli della blockchain, o comunque necessariamente collegati a tale tecnologia».

[36] Lo mette in evidenza A. Federico, *Equilibrio e contrattazione algoritmica*, in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità,* Atti del 15° Convegno Nazionale, Napoli, 2020, p. 85 ss., ma spec. p. 104 s. e altresí A.M. Benedetti, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 415 anche in P. Perlingieri, S. Giova e I. Prisco (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, cit., p. 69 ss.

ISBN 978-88-495-5568-4

viene definito da una confortante formula legislativa come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti» e «la cui esecuzione vincola automaticamente due o piú parti sulla base di effetti predefiniti dalle stesse»[37].

Tale dato normativo va interpretato nel senso che le parti si limitano ad assegnare ad un programma da loro costruito o scelto la realizzazione dei propri interessi: ciò significa che nell'àmbito dell'intera operazione negoziale la fase di formazione del contratto rimane affidata alle parti le quali ricorrono allo *smart contract* nella fase di esecuzione e gestione del regolamento contrattuale[38].

Nell'àmbito dei rapporti della filiera agricola, l'utilizzo della tecnologia *blockchain* garantirebbe la permanenza e la condivisione tra i vari operatori della catena alimentare delle informazioni relative alle caratteristiche e al percorso seguíto dal prodotto, *i.e.*, la sua tracciabilità.

Del pari, anche lo *smart contract* appare un utile strumento di esecuzione dell'intesa negoziale, essendo vòlto a semplificare e a velocizzare le transazioni all'interno della filiera agroalimentare: invero, la trasposizione dell'accordo tra due o piú parti in un linguaggio alfanumerico programmato in base alla logica condizionale «*if this/than that*», risulterebbe funzionale a garantire una maggiore certezza dei traffici giuridici, e, di conseguenza, si attenuerebbe il rischio di inadempimento[39].

4. Il quadro cosí delineato si presta, nondimeno, ad alcune riflessioni.

Di là dagli indiscussi vantaggi offerti dalle soluzioni tecnologiche nel settore agroalimentare, emergono dei profili di criticità che, allo stato attuale, contribuiscono a ingenerare una certa dose di scetticismo mista all'entusiasmo innescato dalla digitalizzazione.

Piú in particolare, con riferimento alle misure tecnologiche di carattere applicativo illustrate, se è vero che consentono di ottimizzare la gestione

[37] Essi «soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con Linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione» (Art. 8 *ter*, comma 2, d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla l. 11 febbraio 2019, n. 1).

[38] Questo determina la distinzione tra la negoziazione algoritmica finalizzata alla formazione del contratto o alla determinazione dell'oggetto e lo *smart contract* funzionale all'esecuzione e alla gestione del rapporto contrattuale: «la macchina prende in carico lo scambio e lo esegue», M. Maugeri, Smart Contracts *e disciplina dei contratti.* Smart Contracts and Contract Law, Bologna, 2021.

[39] E. Maio, La *gestione dell'inadempimento contrattuale negli* smart contract, cit., p. 1340; G. Marino, *L'innovazione tecnologica nella filiera agroalimentare a tutela del consuma-attore*, in *4clegal.com* e A.M. Benedetti, *Contratto, algoritmi e diritto civile transnazionale*, cit., p. 421, il quale rileva che «l'automazione può perfino eliminare la possibilità tecnica di un "inadempimento", blindando l'esecuzione del contratto».

 ISBN 978-88-495-5568-4

della produzione agricola, è altresí vero che esse riducono notevolmente il capitale umano; in piú, l'applicazione stessa di tali misure necessita di nuove figure professionali contrassegnate da competenze e conoscenze altamente specializzate al fine di dare effettivo corso al processo di transizione ecologica e digitale nel settore agricolo.

Quanto all'utilizzo della tecnologia *blockchain* e dello strumento dello *smart contract*, se da un lato manifestano un innegabile punto di forza per la tracciabilità della filiera e per l'automatismo degli effetti predeterminati dalle parti, dall'altro lato occorre far notare, innanzitutto, che dietro al funzionamento di tali tecnologie vi è pur sempre l'opera dell'uomo che provvede all'inserimento dei dati, il che significa che è necessario prevedere un sistema che impedisca la loro manomissione la quale, altrimenti, vanificherebbe l'obiettivo della genuinità e della tracciabilità della filiera.

Inoltre, non è da sottovalutare la questione relativa alla gestione delle sopravvenienze contrattuali al centro del dibattito dottrinale e giurisprudenziale a causa della compatibilità dei rapporti di durata – tra i quali i contratti di cessione di prodotti agricoli e alimentari – a probabili sopravvenuti mutamenti, nella fase di esecuzione del rapporto, delle condizioni sussistenti al momento della costituzione del vincolo contrattuale, idonei ad alterarne l'equilibrio[40].

Nella contrattazione tradizionale, al fine di riequilibrare l'assetto negoziale per renderlo nuovamente soddisfacente agli interessi perseguiti dai contraenti, sono previsti meccanismi rimediali ora legali, ora convenzionali o giudiziali la cui adeguatezza va valutata tenuto conto del singolo rapporto contrattuale nonché dell'esigenza di realizzare i risultati prefigurati dai contraenti mediante quella determinata operazione negoziale[41].

Tale assunto, calato nel fenomeno degli *smart contracts*, è destinato a delineare contorni tutt'altro che definiti, alimentando, invero, profili di incertezza. In particolare, la rigidità insita nella logica condizionale «*if this/than that*», in base alla quale il programma negoziale viene eseguito lungo le direttive analiticamente predeterminate dai contrenti, se da un lato eliminerebbe *ab origine* o quantomeno ridurrebbe grandemente il rischio delle sopravvenienze, dall'altro, ben può accadere che le parti non abbiano previsto tutte le possibili variabili dello svolgimento del rapporto contrattuale, con la conseguenza che la rigidità del sistema informatizzato non consente

[40] Sul tema delle sopravvenienze contrattuali, tra gli altri, si v. F. Macario, *Adeguamento e rinegoziazione nei contratti a lungo termine*, Napoli, 1996; R. Tommasini, *Sopravvenienze e dinamiche di riequilibrio tra controllo e gestione del rapporto contrattuale*, Torino, 2003 e O. Clarizia, *Sopravvenienze non patrimoniali e inesigibilità nelle obbligazioni*, Napoli, 2012.

[41] Sull'apparato rimediale in materia di sopravvenienze, di recente, E. Tuccari, *Sopravvenienze e rimedi nei contratti di durata*, Padova, 2018.

ISBN 978-88-495-5568-4

alcun intervento sulla fase di esecuzione del programma negoziale dato che quest'ultima è totalmente automatizzata.

Pertanto, se è vero che il ricorso allo strumento dello *smart contract* garantisce maggiore rapidità e certezza nei rapporti della filiera, riducendo il rischio di inadempimento grazie alla cristallizzazione della volontà negoziale, è altresí vero che tale rigidità manifesta un evidente punto di debolezza nelle ipotesi di eventuali contingenze sopravvenute, posto che le parti non possono intervenire sul regolamento contrattuale, e, quindi, ad esse è preclusa la facoltà di modifica quale espressione fondamentale dell'autonomia privata[42].

Inoltre, si pone un problema di coordinamento tra il meccanismo di funzionamento della tecnologia a catena di blocchi e la disciplina prevista dal GDPR (Reg. UE 679/2016) in materia di protezione dei dati personali.

In particolare, alla base del corretto funzionamento della *blockchain* vi è la connaturata immutabilità e trasparenza dei dati inseriti: essi restano a disposizione di tutti i partecipanti della filiera; al contrario secondo il GDPR tali dati dovrebbero essere completamente rimossi a richiesta del singolo interessato.

In conclusione, i profili di criticità derivanti dall'impiego delle nuove tecnologie nel settore agricolo in particolare ma in generale nei vari settori rappresentano «un rivoluzionario banco di prova»[43] per il diritto chiamato ad individuare la soluzione piú adeguata ai nuovi problemi emergenti secondo un approccio sistematico funzionale a garantire il giusto equilibrio tra i diversi interessi pratici da soddisfare[44], nel rispetto dei princípi e dei valori identificativi del sistema ordinamentale[45].

Tra l'altro, la velocità di avanzamento del progresso tecnologico non

[42] Sull'autonomia privata quale strumento per il perseguimento di interessi che siano conformi ai valori dell'ordinamento, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, IV, cit., p. 1 ss.

[43] P. Femia, *Introduzione*, in G. Teubner, *Soggetti giuridici digitali? Sullo* status *privatistico degli agenti* software *autonomi*, a cura di P. Femia, Napoli, 2019, p. 9.

[44] P. Perlingieri, *Equilibrio normativo e principio di proporzionalità nei contratti*, in *Rass. dir. civ*., 2001, p. 334 ss. e P. Femia, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile*, Napoli, 1996, pp. 158 ss. e 516 ss.

[45] Per tutti, P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti,* II, *Fonti e interpretazione*, 4ª ed., Napoli, 2020, p. 391, secondo il quale «il bilanciamento dei valori si attua per definizione in riferimento ad un caso concreto, la valutazione del quale vi concorre in forma decisiva» e, ampiamente, G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, p. 1 ss. e spec. p. 120, il quale rammenta che la ragionevolezza è lo strumento capace di «coniugare generalità e particolarità, caso concreto e sistema, al fine di contemperare gli interessi coinvolti e protetti e assicurare la congruenza della regola da applicare alle ragioni del caso concreto», ma anche utile a conciliare «la decisione con i valori riconosciuti dall'ordinamento giuridico (a livello costituzionale, europeo e internazionale)».

 ISBN 978-88-495-5568-4

consente di ritenere risolutivi i risultati raggiunti, sí che «ogni tentativo compiuto dai giuristi per comprendere [i nuovi fenomeni innescati dalla tecnologia] e di disciplinarli rischia di risultare obsoleto nel momento stesso in cui viene svolto»[46].

[46] F. Di Ciommo, Smart contract *e (non-) diritto*, cit., pp. 267 ss. e 291.

ISBN 978-88-495-5568-4

PARTE II

L'identità personale nella società digitale
IoT & Human Enhancement Technologies
Catania, 4 maggio 2023

Gaetano Guzzardi

Tutela della persona e sviluppo tecnologico nella società dell'informazione

Sommario: 1. Transizione digitale e regolazione giuridica. – 2. Contendibilità del mercato digitale ed economia reputazionale. – 3. Conoscenza predittiva e attività di profilazione. – 4. Il valore di scambio dei dati (personali) digitali.

1. La diffusione delle nuove tecnologie ha stravolto, in brevissimo tempo, le tradizionali logiche di mercato e riscritto la geopolitica dell'economia mondiale, con un ripiegamento in favore di quei pochi *players* che hanno saputo, prima d'altri, predire e interpretare le potenzialità e i possibili sviluppi della *digital economy*, trovandosi ben presto a operare, nei rispettivi campi d'elezione, in regime di sostanziale monopolio, per la disponibilità di ingentissime risorse economiche, ma prima ancora per essere riusciti, repentinamente, a divenire monopsonisti della tecnologia di riferimento e del *know how* necessario[1].

Non esiste oggi settore dell'economia mondiale che non sia interessato dalla c.d. rivoluzione digitale e che non sia stato chiamato a rivedere processi, modelli di *business*, canali di approvvigionamento e di vendita, da un lato, per adeguarsi ai cambiamenti imposti da un mondo sempre più globalizzato che volge dall'analogico al digitale, dall'altro, per profittare, inevitabilmente, delle utilità che questa transizione è in grado di apportare.

Quando nel 1979 Michael Aldrich inventava lo *shopping online*, nel 1981 Thomson Holidays realizzava la prima transazione elettronica *BtoB online* o nel 1984 la settantaduenne Mrs. Snowball concludeva il primo acquisto elettronico di generi alimentari tramite la pressione di tasti sul telecomando della TV connessa alla linea telefonica, il diritto risultava pressoché estraneo a tali dinamiche. Non molto dissimile poteva ritenersi la situazione, agli inizi del XXI secolo, quando un gruppo di scienziati del *Georgia Tech* collaborò alla realizzazione di un progetto chiamato *Aware Home*, con l'obiettivo, attraverso una rete di sensori consapevoli, di creare un sistema di interscambio tra abitanti dell'immobile e piattaforma digitale. A quel tempo, anche in considerazione della crescente attenzione al tema della *privacy*, si pensava che la persona che avesse deciso di digitalizzare la propria

[1] Ampie indicazioni sul punto in questo volume nel contributo di M. Ziccardi, *Digitalizzazione e innovazione tecnologica nei contratti di filiera agroalimentare*.

 ISBN 978-88-495-5568-4

sfera personale, e nel caso di specie lo spazio domestico, avrebbe detenuto i diritti esclusivi sulla conoscenza ricavata da simili dati; a distanza di poco più di due decenni appare evidente come il progetto commerciale alla base del c.d. *capitalismo della sorveglianza* riservi un ruolo subalterno al diritto alla *privacy*, prevedendo una gestione delle esperienze degli utenti nello spazio digitale quantomeno condivisa con il gestore dell'infrastruttura[2].

L'ambizione di taluni capitalisti della società digitale, non a caso, sarebbe quella di dar luogo a un *lawless space*, in ragione della sostanziale assenza di confini e dello svolgimento delle dinamiche relazionali (abbiano esse contenuto patrimoniale o non patrimoniale) in uno spazio virtuale, caratterizzato dall'assenza di territorialità e, quindi, di sovranità degli Stati[3]. L'insopprimibile bisogno di assicurare tutela alla persona in qualsiasi situazione di interesse giuridicamente rilevante essa sia coinvolta – a prescindere se si sviluppi in uno spazio fisico o virtuale –, ha ben presto reso evidente come la stessa fosse niente più che una provocazione. Innegabile, ciononostante, è il ritardo con cui gli Stati hanno preso contezza delle proporzioni del fenomeno digitale e dell'impatto che esso ha avuto sull'economia mondiale[4].

[2] S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poveri*, trad. it. a cura di P. Bassotti, Roma, 2019. In questo volume, al riguardo, si v. i contributi di G. Marino, *Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati* e di G. Versaci, *La regolazione dei dati per l'agricoltura di precisione tra questioni generali ed esigenze settoriali.*

[3] J.P. Barlow, *A Declaration of the Independence of Cyberspace*, 8 February 1996, in cui, riferendosi ai governanti della terra, con fare irriverente, espressamente riferiva: «*On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather*»; ampiamente, D.J.B. Svantesson, *Digital contracts in global surroundings*, in S. Grundmann (a cura di), *European contract law in the digital age*, Cambridge-Antwerp-Portland, 2018, p. 51 ss. Sull'ambizione dei capitalisti della sorveglianza ad avere uno spazio digitale senza regole anche S. Zuboff, *op. cit*., p. 114 ss.; nonché E. Schmidt e J. Cohen, *The New Digital Age: Transforming Nations, Businesses, and Our Lives*, New York, 2013, p. 1, ove espressamente si definisce il mondo online come lo spazio senza governo più grande del mondo. Per una disamina delle possibili ricadute giuridiche cfr. E. Battelli, *Questioni aperte in materia di contrattazione nelle piattaforme online*, in *Contratti*, 2022, p. 565 ss.; A.M. Gambino e M. Manzi, *Intelligenza artificiale e tutela della concorrenza*, in *Giur. it*., 2019, c. 1744 ss.; L. D'acunto (a cura di), *Net (or not) Neutrality? Web e regolazione*, Napoli, 2017, p. 19 ss.; già K. Zhu, *Bringing Neutrality to Network Neutrality*, in *Berkeley Technology Law Journal*, 22(1), 2007, *Annual review of law and technology*, p. 627 ss. Per un'indicazione circa la posizione della giurisprudenza comunitaria sul punto (e, in particolare, di Corte giust., 15 settembre 2020, c. riunite 807/18 e 39/19, *Telenor Magyarország Zrt. / Nemzeti Média- és Hírközlési Hatóság Elnöke*) v. S. Poma, *L'interpretazione del regolamento 2015/2120 tra principio di neutralità della rete*, *principio di non discriminazione e Internet aperta*, in *Medialaws*, 2021, 3, p. 227; G. D'Ippolito e M. Monti, *Net neutrality e "tariffe zero": la convergenza delle esigenze democratiche e di mercato, ibidem*, 1, p. 256 ss.

[4] Una panoramica sul grado di digitalizzazione degli Stati dell'Unione e sull'impatto dell'economia digitale sul PIL, in questo volume, nel contributo di A. Scuderi, *La* digital trasformation *nel sistema agroalimentare.*

ISBN 978-88-495-5568-4

Superata una prima fase di colpevole attesa e di sostanziale *deregulation*, non può certo dirsi che la reazione dei principali ordinamenti democratici e delle economie mondiali sia animata da medesime preoccupazioni e dal perseguimento di obiettivi comuni. A un prevedibile approccio, di stampo nordamericano, imperniato sulla dottrina del *laissez-faire* di *smithiana* memoria, le Istituzioni comunitarie manifestano comprensibili riserve, in ragione di forti preoccupazioni per la concorrenzialità dei mercati, la tutela dei consumatori e, in termini più generali, della stessa persona umana.

La Commissione europea, dal canto suo, con una comunicazione del 19 dicembre 2020 dal titolo (e forse anche dal contenuto) fortemente evocativo "*Plasmare il futuro digitale dell'Europa*", in ragione delle nuove sfide poste dalla rivoluzione digitale e della necessità di mantenere sempre un virtuoso equilibrio tra progresso tecnologico e tutela della dignità della vita umana, nel presentare la propria "strategia globale di cooperazione digitale" e le azioni intraprese, ha inteso richiamare l'attenzione delle Istituzioni comunitarie e dei vari *stakeholders* sui cambiamenti imposti dalle tecnologie digitali alla nostra vita quotidiana, al modo in cui concludiamo affari, lavoriamo, interagiamo con gli altri. Tutto ciò nell'àmbito di un articolato programma di interventi sul tema dell'economia digitale, dal quale, almeno in termini programmatici, netta appare la presa di posizione per assicurare una trasformazione digitale plasmata da un'economia forte, competitiva e imperniata sui valori europei[5].

Pochi giorni prima, il 15 dicembre 2020, la stessa Commissione europea presentava due proposte di regolamento (*Digital Service Act* e *Digital Market Act*) per favorire la creazione di un mercato unico digitale a tutela degli interessi economici e dei diritti fondamentali dei cittadini UE, nella consapevolezza di dover adeguare alle trasformazioni del web i regolamenti europei, sostanzialmente fermi agli anni 2000[6]. Proposte di regolamentazione queste ultime pressoché integralmente recepite dai regolamenti del Parlamento europeo e del Consiglio nn. 2022/1925 del 14 settembre 2022, relativo a "mercati equi e contendibili nel settore digitale" (DMA) e 2022/2065 del 19 ottobre 2022, inerente alla creazione di un "mercato unico dei servizi digitali" (DSA).

Non è certo casuale che il Parlamento europeo e il Consiglio, dopo un dibattito durato anni, approvino il primo dei suddetti regolamenti nello

[5] Comunicazione della Commissione UE del 19 febbraio 2020, COM(2020) 67 final, ripresa e integrata nei contenuti, prima dalla *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale* del 26 gennaio 2022 e, da ultimo, nella dichiarazione strategica *Decennio digitale europeo: obiettivi digitali per il 2030*, tutte consultabile sul sito istituzionale dell'Unione europea.

[6] Il riferimento, in particolare, è alla direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000, relativa a «taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno» (c.d. direttiva sul commercio elettronico).

 ISBN 978-88-495-5568-4

stesso giorno in cui il Tribunale UE pubblicava la controversa decisione sul caso *Google Android*[7]; buona parte delle condotte contestate al colosso di *Mountain View* vengono, difatti, rappresentate, al considerando n. 3, come condizioni strutturali del mercato dei "servizi di piattaforma di base", in cui «un numero ridotto di grandi imprese», in ragione del considerevole potere economico detenuto, «esercitano un controllo su interi ecosistemi di piattaforme nell'economia digitale».

Con l'approvazione del *Digital Market Act* il legislatore comunitario, in particolare, ha inteso definire regole basilari di funzionamento del mercato digitale, per scoraggiare condotte anticoncorrenziali, consentire agli utenti di accedere alle piattaforme digitali in condizioni di sicurezza e agli operatori commerciali di operare in modo libero ed equo, alla stregua di quanto è possibile fare in ambiente *offline*[8].

Evidente pare il tentativo del legislatore comunitario, nella consapevolezza che la tecnologia è una «realtà invadente»[9], di provare a guidare (pur senza con ciò voler arrestare) il progresso tecnologico, così da assicurare ai cittadini dell'Unione, innanzitutto, la possibilità di scegliere liberamente e in sicurezza, prendendo decisioni migliori sulla base delle informazioni provenienti dal trattamento dei dati di navigazione degli stessi, che dovrebbero, difatti, essere accessibili a tutti e non nella disponibilità di pochi e le cui modalità e finalità di raccolta dovrebbero essere rese trasparenti, così permettendo a tutti gli utenti di poter trarre il massimo vantaggio dall'innovazione e dalla concorrenza e all'Europa – incalza la Commissione UE – di esprimere il meglio dei propri valori: apertura, equità, pluralismo, democrazia e sicurezza[10].

[7] Il riferimento è al caso Trib. UE, 14 settembre 2022, c. 604/18, *Google e Alphabet c. Commissione*, per cui sia consentito il rinvio a G. Guzzardi, *L'abuso di posizione dominante nel mercato dei servizi digitali,* in *Nuova giur. civ. comm*., 2023, p. 309 ss.

[8] Tra i principali divieti, non a caso, si rilevano quelli di non discriminazione a favore dei propri servizi, di garantire l'interoperabilità con la propria piattaforma ad altre concorrenti, di condividere, nel rispetto delle norme sulla privacy, i dati che vengono forniti o generati attraverso le interazioni degli utenti commerciali e dei loro clienti sulla piattaforma dei *gatekeeper*, con sanzioni sino al 10% del fatturato e, addirittura, di natura straordinaria quali l'obbligo di cessione di parte degli *asset* aziendali o delle proprietà aziendali (*splitting*).

Con il pacchetto del *Digital Services Act*, invece, in particolare, si intende monitorare *ex ante* le attività delle piattaforme online che agiscono come *gatekeeper*, prevedendo specifici obblighi e divieti per scongiurare una serie di pratiche sleali; assicurare proporzionalità nell'intervento di disciplina dei servizi digitali, prevedendo regole diverse in ragione del ruolo, delle dimensioni e dell'impatto che i diversi operatori hanno sull'ecosistema digitale (servizi di intermediazione, di *hosting*, di *cloud*); regole *ad hoc* sono previste per le piattaforme che raggiungono più del 10% dei 450 milioni di consumatori europei.

[9] A. Gorassini, Lo *spazio digitale come oggetto di un diritto reale?*, in *Medialaws*, 2018, p. 54.

[10] In questa direzione, significativa importanza assume l'approvazione (il 14 giugno 2023), a larga maggioranza, da parte del Parlamento europeo, del testo definitivo ed emen-

ISBN 978-88-495-5568-4

Nonostante i significativi passi in avanti degli Stati e della stessa UE per assicurare una equilibrata regolamentazione delle operazioni economiche concluse nello spazio digitale e che, in particolare, coinvolgano i consumatori, è indubbio come le attuali risposte alle istanze di tutela siano ancora assolutamente insufficienti e inadeguate.

La pandemia di Covid-19, tra l'altro, ha fatto registrare un aumento del 60% dell'uso di *internet*, determinando un avvicinamento al mondo del *web* anche di persone prima del tutto disinteressate o incapaci di approcciarsi, anticipando di almeno cinque anni la transizione digitale rispetto ai tempi previsti, così rendendo ancor più urgenti interventi di armonizzazione o, in ogni caso, l'individuazione di regole certe e funzionali da parte degli Stati. L'impossibilità, in tempo di pandemia, di ricorrere ai canali di approvvigionamento tradizionali, incompatibili con il distanziamento, ha altresì avuto l'effetto anche di accelerare il consolidamento della posizione dominante dei *tech giants*, al punto da risultare imprescindibili per la stessa erogazione di alcuni servizi essenziali o il soddisfacimento di bisogni primari per lo sviluppo della persona, basti pensare allo svolgimento di attività lavorative (*smart working*), di istruzione e formazione (*e-learning*) e di talune prestazioni sanitarie (*eHealth*)[11].

dato (c.d. *AI Act*) della *Proposta di Regolamento del Parlamento europeo e del Consiglio 2021/0106* del 21 aprile 2021, che stabilisce regole armonizzate sull'IA, la cui entrata in vigore è attesa entro la primavera del 2024. Il provvedimento, infatti, oltre a imporre che, nel caso di utilizzo di sistemi di intelligenza artificiale generativa (come *ChatGPT, Bard*), risulti esplicito che i relativi *output* siano stati "generati da IA", procede, secondo un sistema *risk-based approach*, a una classificazione delle applicazioni di IA in quattro livelli di rischio, qualificando di rischio "inaccettabile" – al punto da vietarli – tutti quei sistemi di IA che, tra l'altro, possano costituire una violazione dei diritti fondamentali, determinare una "manipolazione comportamentale cognitiva di persone o gruppi vulnerabili specifici" o, ancora, il riconoscimento delle emozioni con finalità di polizia o in ambiente scolastico o lavorativo. Tra le prime riflessioni in merito, oltre ai già citati contributi di G. Marino e G. Versaci in questo volume (e, sul punto, si cfr. anche quello di E. Tuccari, *Note minime sull'asistematica disciplina del* neuromarketing), v. G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti",* in *Riv. dir. civ*., 2021, p. 850 ss.; D. Messina, *La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una "discutibile" tutela individuale di tipo consumer-centric nella società dominata dal "pensiero artificiale"*, in *Medialaws*, 2022, 2, p. 196 ss.; S. Orlando, *Per un sindacato di liceità del consenso privacy*, in *Persona e mercato*, 2022, p. 539; Id., *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di artificial intelligence act*, *ivi*, p. 346 ss.; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea,* in *Riv. dir. civ*., 2020, p. 1246 ss., anche per una panoramica sul dibattito sviluppatosi in proposito nella letteratura europea e sul primo approccio delle Istituzioni comunitarie.

[11] A.M. Gambino e R. Giarda, *L'accesso ad Internet come diritto*, in *Medialaws*, 2021, pp. 105 s., 118; Corte giust. UE, 15 settembre 2020, c. riunite 807/18 e 39/19, cit.; Cass., 27 agosto 2020, n. 17894, in *OneLegale*, la quale, sebbene non si occupi espressamente del diritto all'accesso a internet offre spunti per la verifica dei termini utili per la riconducibilità di un nuovo diritto nella categoria dei diritti fondamentali della persona, "catalogo aperto"

 ISBN 978-88-495-5568-4

Contestualmente alla crescente diffusione dell'*e-commerce* – espressione della capacità di riorganizzazione della catena distributiva (*supply chain*), pilastro della *Strategia per il mercato unico digitale*[12] –, si assiste, infatti, a un progressivo spostamento del potere di mercato dal produttore al distributore e, a sua volta, da quelli che utilizzano canali tradizionali in favore di chi è presente nelle piattaforme *online*, così favorendo, appunto, il passaggio al c.d. *capitalismo digitale*, o con una sineddoche, al capitalismo delle piattaforme digitali.

2. Il mercato digitale, per struttura e conformazione, tende a essere la rappresentazione plastica delle teorie neoliberiste; tuttavia, pur non disconoscendo le positive ricadute in termini di compiuta valorizzazione dell'autonomia negoziale delle parti, quest'ultima non può mai operare in spregio di diritti e libertà fondamentali o di quei valori comuni alle principali democrazie, come la stessa concorrenzialità dei mercati, che, anche in tale peculiare contesto, le Istituzioni di riferimento sono chiamate ad assicurarne la primazia e la piena operatività[13]. Anche al cospetto di una rivoluzione digitale spinta pure dalla "retorica dell'inevitabilismo"[14], infatti, il diritto è chiamato a (continuare a) svolgere il proprio ruolo di regolatore

in continuo aggiornamento in ragione dell'evoluzione normativa e sociale e in cui si annoverano diritti in passato considerati secondari (diritto all'identità personale, all'oblio, alla riservatezza, all'identità digitale, etc.). Non tutte le volte in cui la tecnica renda possibili nuovi *commoda*, tuttavia, la pretesa di avvalersene assurge automaticamente al rango di diritto fondamentale; è necessario infatti che il diritto pertenga alla persona e non al suo patrimonio e che il relativo esercizio non possa essere impedito senza sopprimere o limitare la dignità e la libertà dell'essere umano. Nel caso di specie, la Corte non riconobbe nel diritto all'accesso a un servizio di telefonia i termini di un diritto fondamentale, non essendo lo stesso necessario alla sopravvivenza; ad analoghe conclusioni potrebbe pervenirsi con riguardo al diritto di accesso a internet, senz'altro di rilievo, ma non per questo ascrivibile nel novero dei diritti fondamentali della persona.

[12] Comunicazione della Commissione UE al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 6 maggio 2015, consultabile sul sito istituzionale della Commissione.

[13] Sul punto si osservino le considerazioni svolte dal Gruppo di ricerca sul diritto dei servizi digitali in 2015, fondato a Osnabrück, sotto l'egida del *European Law Institute* (ELI) e contenute nel report, Aa.Vv., *Discussion Draft of a Directive on Online Intermediary Platforms*, in *Journal of European Consumer and Market Law*, 2016, p. 164 ss.; nonché in dottrina C. Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, p. 379 ss.; G. Finocchiaro, Il *quadro d'insieme sul Regolamento europeo*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, diretto da Id., Bologna, 2017, p. 3.

[14] Significativi gli investimenti della *Silicon Valley* per l'affermazione di una "ideologia inevitabilista" circa l'inarrestabilità della diffusione delle nuove tecnologie e l'imminente transizione alla computazione ubiqua, in cui tutto sarà connesso, informatizzato e, dunque, processabile; sul punto G. Dublon e J.A. Paradiso, *Extra Sensory Perception*, in *Scientific American*, 17 giugno 2014; E. Schmidt e J. Cohen, *op. cit*., p. 156.

ISBN 978-88-495-5568-4

dei conflitti sociali, provando a contenere anche quella realtà che, allo stato, sembra superare la fantasia, così da assicurare sempre un equilibrato bilanciamento tra progresso tecnologico, tutela dell'essere umano e del diritto all'autodeterminazione, la cui crescente rilevanza e portata espansiva è indissolubilmente connessa ai mutamenti sociali e culturali[15].

Istanze di tutela provengono da pressoché tutte le categorie di utenti digitali, sottoposti a una regolamentazione algoritmica che assume i tratti di una algocrazia nelle mani di pochi (i c.d. *Gafam*), i quali, peraltro, detenendo sia il potere economico sia quello tecnologico, hanno assunto un ruolo nevralgico anche nel dibattito politico mondiale[16]. I *social network*, nuove agorà di ogni comunità in cui condividere informazioni, esprimere opinioni, lanciare campagne pubblicitarie, ad esempio, sono rapidamente divenuti lo strumento più efficace per raggiungere il maggior numero di persone nel minor tempo possibile, tanto da essere utilizzati anche dalle stesse Istituzioni pubbliche per diramare comunicati e anticipare il conte-

[15] Ampiamente S. Rodotà, *Dal soggetto alla persona*, Napoli, 2007; Id., *Il nuovo Habeas corpus: la persona costituzionalizzata e la sua autodeterminazione*, in S. Rodotà e M. Tallacchini (a cura di), *Ambito e fonti del biodiritto*, I, in *Tratt. di biodiritto Rodotà e Zatti*, Milano, 2011, p. 211 ss.; C. Castronovo, *Autodeterminazione e diritto privato,* in *Eur. dir. priv*., 2010, p. 1047; più di recente C. Irti, Il *danno non patrimoniale da lesione del diritto all'autodeterminazione: danno in re ipsa?,* in *Giur. it*., 2019, c. 288 ss.; I. Rapisarda, *Consenso informato e autodeterminazione terapeutica*, in *Nuove leggi civ. comm*., 2019, p. 43 ss.; diffusamente Ead., *Il diritto sul corpo nell'era biotecnologica*, Catania, 2023. Sul complesso (quanto inevitabile) rapporto tra diritto e tecnica, anche al fine di pervenire a una equilibrata allocazione dei rischi e imputazione delle responsabilità connesse allo sviluppo tecnologico G. Di Rosa, *Profili giuridici dell'esistenza*, Torino, 2022, pp. 153 ss., 174 ss.; Ar. Fusaro, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *Nuova giur. civ. comm*., 2020, p. 1344 ss.; E. Palmerini, *Soggettività e agenti artificiali: una soluzione in cerca di un problema?*, in *Oss. dir. civ. comm*., 2020, p. 445 ss.

[16] M. Sciacca, *Algocrazia e sistema democratico. Alla ricerca di una mite soluzione antropocentrica*, in *Contr. impr*., 2022, p. 1173 ss. Con l'espressione *Gafam* si è soliti fare riferimento al sostanziale regime di oligopolio imposto dai colossi della tecnologia digitale (Google, Amazon, Facebook, Apple, Microsoft), che, secondo Peter Thiel, co-fondatore di Pay-pal e tra i maggiori finanziatori esterni di Facebook, risulterebbe addirittura una caratteristica intrinseca della nuova economia digitale, e non un effetto indesiderato, perché se non fossero state queste aziende così dominanti non avrebbero mai avuto così tanto denaro da spendere in innovazione, contribuendo al raggiungimento di un tale progresso tecnologico. Un primo tentativo di regolamentazione, nel panorama europeo, dell'attività di tali "guardiani dell'accesso alla rete", detti anche "*LoPs - Large Online Platforms*", come detto, si deve al reg. (UE) 2022/1925. La relativa individuazione, ad opera dell'art. 3, avviene su base presuntiva, nel caso in cui, per volumi di fatturato, capitalizzazione di mercato e numero di utenti finali fissati al § 2, l'impresa sia in grado di determinare un significativo impatto sul mercato interno; operi quale piattaforma di base, risultando strategica per altre imprese per interagire con gli utenti finali, nonché detenga una posizione consolidata e duratura, nell'àmbito delle proprie attività, o è prevedibile possa assumerla nel prossimo futuro. Per ulteriori indicazioni in proposito sia consentito il rinvio a G. Guzzardi, *L'abuso*, cit., p. 316 ss.

 ISBN 978-88-495-5568-4

nuto di provvedimenti e atti normativi[17]; allo stesso tempo, però, costituiscono una delle principali fonti di approvvigionamento di dati utili sugli interessi personali e di consumo degli utenti, tanto da riservarsi i *gatekeeper* amplissime "licenze d'uso" dei dati estratti per l'esercizio di prerogative anche a finalità commerciale[18].

La strategia delle principali piattaforme digitali, come si vedrà meglio *infra*, mira a generare introiti non attraverso la concessione a titolo oneroso di prodotti o servizi digitali, bensì incrementando il più possibile il traffico di dati sulla propria piattaforma, così da massimizzare i profitti provenienti dagli annunci pubblicitari collegati alle ricerche degli utenti[19]. Il profitto immaginato dall'impresa che offre i servizi digitali è strettamente connesso alla possibilità di trattenere i dati personali degli utenti, da mettere a disposizione degli investitori pubblicitari e delle imprese operanti nel settore della comunicazione commerciale previo trattamento e profilazione.

Il mercato digitale appare così riconducibile a quelli che si è soliti definire "*business zero-price*", in ragione della (supposta) gratuità dei beni e servizi offerti per l'assenza di una controprestazione in denaro dell'utente[20].

[17] Secondo alcuni studi che necessitano, però, ancora di validazione, taluni algoritmi alla base del funzionamento di alcune piattaforme e social network di larga diffusione sarebbero stati progettati per poter funzionare in maniera differente a seconda della parte del mondo in cui verrebbero utilizzati o del target di utenti che vi accedono, al punto che potrebbero proporre, ad esempio, contenuti privi di alcuna utilità e valore sociale in una certa parte del mondo al deliberato scopo di influenzarne negativamente le coscienze e, al contempo, promuovere contenuti e temi in grado di arricchire il bagaglio di conoscenze e stimolare la riflessione critica degli utenti nella parte opposta del mondo, così potendo risultare potenti mezzi di indottrinamento delle masse e di condizionamento, in particolare, delle categorie più vulnerabili su temi sensibili anche alle politiche governative. Sulla c.d. "vulnerabilità digitale" dei minori e sull'impatto delle nuove tecnologie nella formazione della personalità degli stessi R. Senigaglia, *Il dovere di educare i figli nell'era digitale,* in *Persona e mercato*, 2021, pp. 512, 519 ss. Sulle possibili applicazioni discriminatorie della tecnologia algoritmica, alle indicazioni di cui alla nota 32, *adde*, A. Neri, *Uso di un algoritmo discriminatorio nella contrattazione privata,* in *Nuova giur. civ. comm*., 2021, p. 983 ss.; Aa.Vv., *Fairness and Non-Discrimination*, in *Responsible AI: A Global Policy Framework,* consultabile all'indirizzo *itechlaw.org*, 2021, p. 51 ss.

[18] C. Perlingieri, *Profili civilistici dei social networks*, Napoli, 2014, p. 88 ss.; più di recente G. Marino, *Mercato digitale e sistema delle successioni mortis causa*, Napoli, 2022, p. 20 ss.

[19] Per una disamina delle ricadute sulla stessa contendibilità del mercato di riferimento di tali scelte commerciali si rinvia ancora a G. Guzzardi, *L'abuso*, cit., 309 ss., ove un approfondimento sulla strategia di Google finalizzata a massimizzare i propri introiti in ragione dell'implementazione di tecniche di aggressione del mercato di riferimento volte a incrementare, in maniera massiva, il traffico di dati sulla propria piattaforma in ragione dell'integrazione di plurimi servizi e prodotti del c.d. "ecosistema Google".

[20] Sul carattere soltanto apparente della gratuità di tale scambio A. De Franceschi, *Il "pagamento" mediante dati personali*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1382; M. Gal e D.L. Rubinfeld,

ISBN 978-88-495-5568-4

Se ciò non impedisce, da un lato, alle Autorità *antitrust* europee di ritenere immutata la patrimonialità dello scambio, per la sussistenza di un valore intrinseco dei dati scambiati – peraltro, poi oggetto di cessione (a titolo oneroso) a terzi – e, dunque, che talune pratiche dei *tech giants* possano essere ritenute anticoncorrenziali anche soltanto per la maggiore propensione dei mercati digitali a generare posizioni di monopolio (*winner takes all*)[21], dall'altro, rafforza l'idea che tale spazio di interazione non possa essere analizzato e contestualizzato con parametri tradizionali[22].

La sostanziale assenza di confini fisici della rete, l'estrema dinamicità (sempre in rapida e continua trasformazione) e la presenza di numerosi "mercati comunicanti", anche in ragione del moltiplicarsi delle interazioni tra diversi portatori di interessi[23], generano significative esternalità di rete che contribuiscono a determinare il consolidamento di posizioni dominanti, senza che a ciò debbano necessariamente concorrere intenzionali condotte abusive.

La piena disponibilità della tecnologia di base, in continua evoluzione, e dell'infrastruttura che regge e alimenta il mercato dei servizi nella medesima scambiati, determina importanti effetti di *lock-in*, che assicurano al gestore della piattaforma economie di scala estreme, alimentate anche dalla ricercata continua interazione tra più dispositivi c.d. "intelligenti", sempre intercon-

The Hidden Costs of Free Goods, in *Antitrust Law J*., 2016, p. 540 ss.; V. Zeno Zencovich e G. Giannone Codiglione, *Ten Legal Perspectives on the "Big Data Revolution"*, in F. Di Porto (a cura di), *Big data e concorrenza,* in *Conc. merc*., 2016, p. 40; G. Colangelo, *Big data, piattaforme digitali e antitrust*, in *Merc. conc. reg*., 2016, p. 427. Sul punto, altresì, cfr. la critica posizione di G. Alpa, *Sul potere contrattuale delle piattaforme digitali,* in *Contr. impr*., 2022, p. 723, secondo il quale «i dati personali non possono essere considerati "merce" al pari dei prodotti e dei servizi».

[21] Fenomeno quest'ultimo che si manifesta anche nell'ormai nota pratica di *killer acquisitions* delle *start-up* più promettenti; indicazioni sul punto in M. Ainis, *L'Autorità antitrust alla prova dei mercati digitali,* in *Dir. inf.,* 2022, p. 1; D.S. Evans e R. Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses,* in *Nat. Bur. Econ. Res*., 2013, p. 430 ss. Sulla naturale propensione della rete digitale di favorire dinamiche anticoncorrenziali per cui chi, prima d'altri, acquisisce un posizionamento di vantaggio è in grado di indirizzare il mercato cfr. Quarta e Smorto, *Diritto privato dei mercati digitali*, Firenze, 2020, p. 71; E. Frosini, *Internet e democrazia,* in *Dir. inf.,* 2017, p. 670.

[22] Sia consentito sul punto il rinvio a G. Guzzardi, *L'abuso*, cit., p. 310 ss., ove ulteriori indicazioni su quanto evanescente possa risultare il tentativo di verificare l'eventuale abusività di eventuali posizioni dominanti assunte dai *gatekeeper* facendo ricorso a parametri tradizionali (come, nel caso specifico, a quello della "definizione del mercato rilevante"). Criticità nella definizione del mercato rilevante in tale particolare àmbito già emerse con riguardo al caso *Google Shopping*; sul punto cfr. A.M. Gambino e M. Manzi, *op. cit.,* c. 1747; F. Vessia, *Big data: dai vantaggi competitivi alle pratiche abusive,* in *Giur. comm.*, 2018, I, p. 1066 ss.

[23] Indicazioni in tal senso in E. Camilleri, «*Facebook credits*» *e commercializzazione di beni virtuali per social games: l'abuso di posizione dominante alla prova di un mercato con piattaforma plurilaterale,* in *AIDA*, 2011, p. 146.

 ISBN 978-88-495-5568-4

nessi e in grado di offrire servizi integrati. Risultanze, queste ultime, conseguenza anche dello strapotere tecnologico e finanziario dei *tech giants* che, inevitabilmente, condizionano il funzionamento del mercato unico dei servizi digitali, con evidenti ricadute sugli operatori professionali, ma innanzitutto sul consumatore, fruitore finale dei servizi e dei beni in esso scambiati[24].

Eppure già all'art. 3, § 1, reg. (UE) 2015/2120, con il riconoscimento del diritto degli utenti «di accedere a informazioni e contenuti, (…) di utilizzare e fornire applicazioni e servizi (…) tramite il servizio di accesso a Internet», si avanzava l'idea della necessità di uno spazio digitale libero, non monopolizzabile da "chi arriva prima"[25]. Tutto ciò nell'ottica di favorire la c.d. *net neutrality*, da intendersi come assenza di restrizioni arbitrarie nell'accesso alla rete (e alle informazioni in essa disponibili e veicolate), che ripercussioni determinano non soltanto sul fronte della concorrenza, ma anche della tutela dei diritti e delle libertà fondamentali degli utenti, in virtù del profilarsi di seri rischi per le stesse democrazie mondiali e il pluralismo informativo.

Quello in esame, peraltro, è un mercato in cui significativo rilievo assumono il fattore reputazionale e la c.d. *scelta predefinita*, come rilevato anche nel *leading case Google Android*[26], attesa la propensione dell'utente a fidarsi delle recensioni rilasciate da (e a favore di) altri fruitori del servizio o acquirenti del prodotto e a non modificare le scelte preimpostate dal fornitore dei servizi digitali[27].

Friedrich von Hayek, premio Nobel per l'economia nel 1974, precursore della *sharing economy*, già anticipava dei possibili rischi di un mercato della reputazione (oggi, della recensione) – cliente buono, ospite diligente, fornitore impeccabile, *host* accogliente, tassista invadente –, il cui passo ulteriore è quello verso una "economia comportamentale", apparentemente tesa a sconfiggere i "comportamenti irrazionali"[28], ma della cui attendibilità è lecito dubitare, specie ove gli strumenti e le applicazioni deputate a "correggere" le possibili distonie rilevate (ma rispetto a parametri uni-

[24] G. Alpa, *La legge sui servizi digitali e la legge sui mercati digitali,* in *Contr. impr*., 2022, p. 2.

[25] A.M. Gambino e R. Giarda, *op. cit*., p. 112 s.

[26] La Commissione, in particolare, nel richiamato caso *Google Android* avrebbe constatato una maggiore frequenza di utilizzo delle app *Google* sui dispositivi *Android* se preinstallate rispetto a quelli in cui gli utenti, per assicurarsene l'utilizzo, dovrebbero previamente scaricarli, come nel caso dei dispositivi *Windows Mobile*, ad esempio, in cui risulta preinstallato *Bing*, concorrente motore di ricerca della galassia *Microsoft*. Ulteriori riferimenti in G. Guzzardi, *L'abuso,* cit., p. 313 ss.

[27] Sul determinante ruolo delle recensioni nel mercato dell'online, sorretto da uno «spirito *wiki*», ossia da una collaborazione attiva tra gli utenti, G. Alpa, *Sul potere contrattuale*, cit., p. 723.

[28] F.A. von Hayek, *Competizione e conoscenza*, Soveria Mannelli, 2017, p. 29 ss.; F. Denozza, *Mercato, razionalità degli agenti e disciplina dei contratti*, in G. Gitti e M.R. Maugeri e M. Notari (a cura di), *I contratti per l'impresa*, I, Bologna, 2012, p. 69 ss.

ISBN 978-88-495-5568-4

lateralmente preimpostati dal gestore del servizio), risultino governate da imperscrutabili algoritmi e sistemi di *machine learning*[29].

Il riferimento è a *software* e applicazioni, oggi alimentati anche da sistemi di intelligenza artificiale, che consentono il raggiungimento di prefissati obiettivi secondo la logica apprendimento/assunzione, attraverso reti neurali (*neural networks*) programmate per funzionare sul modello del cervello umano[30]. Non v'è dubbio come l'espressione utilizzata per identificare tali processi, "intelligenza artificiale", si presenti come un evidente ossimoro, perché quantunque con forza intenda mettere in evidenza lo scopo di tale nuova tecnologia, ossia riprodurre la più caratterizzante delle prerogative della specie umana, l'intelligenza, non riesce però a celare come l'imitazione dell'agire umano che ne consegue risulti l'esito di un processo automatizzato e, come tale, sprovvisto di tutte quelle componenti – sensibilità, morale, giudizio, equità, discrezionalità, spontaneità, intuito – che, invece, qualificano e rendono irripetibile la capacità di ragionamento e di giudizio dell'essere umano[31].

La macchina, anche la più sofisticata, allo stato, può anche emettere rapidamente un responso affidabile, ma è carente di trasparenza quanto all'*iter* argomentativo, al ragionamento sotteso, così risultando spesso difficile comprendere il senso di determinate risposte in forza di una opacità di fondo dell'algoritmo di autoapprendimento. Un'intelligenza, quindi, sprovvista di ragione, una elaborazione, quantunque complessa, esito non di connessioni spontanee e indipendenti o deduzioni logiche, bensì dell'applicazione di principi matematici, di un "ragionamento" per mere inferenze statistiche[32].

[29] Non è un caso se nell'àmbito del pacchetto di riforme al vaglio del legislatore comunitario per fronteggiare le distorsioni generate dalla *digital transformation*, come detto, grande sia l'interesse alla definizione di regole armonizzate sull'IA. Ciò, a conferma, da un lato, della centralità assunta dalle tecnologie di IA in molteplici settori strategici per lo sviluppo e la stessa salvaguardia dell'umanità, dall'altro, della fondatezza delle preoccupazioni segnalate dai vari *stakeholders* all'esito dell'ampia consultazione avviata dalla Commissione UE con la pubblicazione del Libro bianco sull'IA. Sulla necessità di assicurare trasparenza e di esplicitare il percorso dell'algoritmo v. G. Alpa, Il *mercato unico digitale,* in *Contr. impr./Eur*., 2021, p. 1 ss.

[30] U. Ruffolo, *L'intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento",* in *Giur. it*., 2021, p. 502.

[31] Sul tema G. Di Rosa, *Quali regole*, cit., pp. 824-825; S. Crisci, *Intelligenza artificiale ed etica dell'algoritmo,* in *Foro amm*., 2018, p. 1787. Con un parere congiunto del 29 maggio 2020, dal titolo "*Intelligenza artificiale e medicina: aspetti etici*", anche il Comitato Nazionale per la Bioetica e il Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita, consultabile all'indirizzo internet *bioetica.governo.it*, hanno avuto modo di evidenziare come obiettivo dell'IA sia proprio quello di imitare, tramite tecnologie informatiche, aspetti dell'intelligenza umana, per sviluppare "prodotti informatici o macchine" in grado sia di interagire e di apprendere dall'ambiente esterno sia di assumere decisioni con crescenti gradi di autonomia".

[32] Sul punto ancora G. Di Rosa, *Profili giuridici*, cit., p. 158 ss.; Id., *Quali regole*, cit., p. 828 ss., ove anche un approfondimento sul caso deciso da Cons. Stato, 8 aprile 2019, n.

 ISBN 978-88-495-5568-4

3. La conoscenza dei *trend* di condotta e di consumo degli utenti permette al *provider*, non soltanto di meglio orientare le proprie scelte commerciali, ma anche di provare ad anticipare (e influenzare) i bisogni degli utenti. L'utilizzo di meccanismi algoritmici di ordinamento in sequenza, valutazione o recensione, difatti, consente ai fornitori di servizi di intermediazione nel mercato digitale di assicurare agli utenti commerciali la massimizzazione dei profitti, proprio in considerazione della capacità di incidere sulle stesse scelte dei consumatori; il c.d. "posizionamento" (non casuale) di beni e servizi da parte delle piattaforme, difatti, è strettamente correlato alla capacità di prevedere il comportamento degli utenti in rete[33].

Il decisivo cambio di passo fatto registrare dai *gatekeeper* nella propria strategia commerciale, non più finalizzata ad estrarre dati comportamentali al mero fine di migliorare il servizio offerto agli utenti, bensì per alimentare un mercato dinamico dell'*advertising online*, se da un lato ha determinato un incredibile ed esponenziale crescita dei volumi di fatturato dei *tech giants*, dall'altro ha reso ancor più percepibili i rischi connessi alle attività di tracciamento, profilazione, manipolazione o *cookies poisoning*. D'altronde, anche all'esito della (pur netta) presa di posizione della Corte di giustizia circa la prevalenza, in linea di principio e salvo ragioni particolari, dei diritti fondamentali degli utenti sanciti agli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE sull'interesse economico del gestore della piattaforma e financo sull'interesse del (grande) pubblico a (continuare ad) accedere a una data informazione, con conseguente obbligo per le piattaforme di assicurare il c.d. *delinking*[34], non può certo dirsi che i colossi del *web* ab-

2270, inerente all'utilizzo dell'algoritmo in procedure valutative della Pubblica Amministrazione; nonché U. Ruffolo, *op. cit*., p. 502; S. Amato, *Biodiritto 4.0 Intelligenza artificiale e nuove tecnologie*, Torino, 2020 p. 100 ss.; E. Pellecchia, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leggi civ. comm*., 2018, p. 1209 ss. Sul carattere discriminatorio dell'algoritmo, oltre a quanto si dirà infra, anche Trib. Bologna, sez. lav., 31 dicembre 2020, in *OneLegale*, chiamato a pronunciarsi sulle modalità di funzionamento dell'algoritmo "*Frank*", programmato per profilare i *riders* della società di consegne *Deliveroo*, secondo un discusso *ranking* reputazionale che, nel tenere conto di parametri quali l'affidabilità e la partecipazione del dipendente, determinava le effettive possibilità di accedere o meno ai turni di lavoro. Come riportato nella ricostruzione in fatto dell'ordinanza, in buona sostanza, financo "l'adesione del rider a forma di autotutela collettiva e, in particolare, ad astensioni totali dal lavoro coincidenti con la sessione prenotata", comportava una penalizzazione del lavoratore.

[33] Sul punto cfr. il considerando 24 reg. (UE) 1150/2019 del Parlamento europeo e del Consiglio del 20 giugno 2019, che promuove equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online.

[34] Il riferimento è a Corte giust., 13 maggio 2014, c. 131/12, *Google Spain c/ Agencia Española de Protección de Datos (AEPD) e M. Costeja Gonzàlez*, in *https://eur-lex.europa.eu*; indicazioni in merito in V. Cuffaro, *Una decisione assennata sul diritto all'oblio*, in *Corr. giur*., 2019, p. 1189 ss.; G. Resta e V. Zeno Zencovich (a cura di), *Il diritto all'oblio*

ISBN 978-88-495-5568-4

biano rivisto le proprie strategie di estrazione e indicizzazione dei dati. Gli stessi vertici della più famosa società di *Mountain View*, nel tranquillizzare gli investitori, ripetendo il *refrain* dell'azienda – secondo il quale compito e intenzione di *Google* sarebbe quello di organizzare tutta l'informazione del mondo per renderla universalmente accessibile a tutti – rilevavano come la decisione della Corte UE non era altro che un danno collaterale dello scontro tra il diritto a essere dimenticati e il diritto alla conoscenza[35].

L'obiettivo (dichiarato) dei *gatekeeper* può anche essere quello di sviluppare conoscenza non per sorvegliare gli utenti o invaderne la *privacy* e la riservatezza, ma è altresì fuor di dubbio che, attraverso l'utilizzo sempre più massiccio di sistemi algoritmici in grado di dedurre pensieri, emozioni, interessi degli utenti, l'intento non sia più (soltanto) quello di assicurarsi una detenzione passiva dei dati accidentalmente rilasciati dagli utenti, utile per monitorare e migliorare i servizi offerti, bensì per trarre profitto dalla vendita di indagini predittive ricavate proprio dalle tracce di navigazione in rete, dal riuso dei c.d. "scarti digitali"[36]. Chiunque navighi nel *web*, infatti, a prescindere da quanto effimera sia l'attività (anche accidentalmente) svolta, lascia tracce, genera "impronte digitali", dalle quali i c.d. capitalisti della sorveglianza sono in grado di poter ricavare conoscenza, un *surplus* comportamentale[37].

Allo scopo di ricavare conoscenza e valore economico mediante l'attività di profilazione, la piattaforma provvede a mettere in collegamento, come tessere di un mosaico, le informazioni estratte[38]; secondo le logiche

su internet dopo la sentenza Google Spain, Roma, 2015, p. 29 ss.; nella giurisprudenza interna, Cass., 24 novembre 2022, n. 34658, in *Giur. it.,* 2023, c. 827.

[35] Sul diritto all'oblio nello spazio digitale cfr. anche la recente decisione del Garante per la protezione dei dati personali del 23 marzo 2023, n. 111, consultabile sul sito istituzionale dell'Autorità, con cui è stato ordinato a Google il *delisting* di URL in ragione dell'assoluzione di un utente dall'accusa di truffa e della necessità di assicurare, appunto, la tutela del diritto all'oblio del medesimo. Sul tema D.G. Ruggiero, *Persona e identità digitale*, Napoli, 2023, p. 192 ss.; A. La Spina, *Complessità e identità personale*, Napoli, 2022, p. 496 ss.

[36] S. Zuboff, *op. cit*., pp. 101, 106; A. McStay, *Emotional AI: The Rise of Empathic Media*, London, Sage, 2018.

[37] S. Zuboff, *op. cit*., pp. 197-198; da ultimo, M. Imbrenda, *Persona e scelte di consumo fra conoscenze neuroscientifiche e nuove frontiere tecnologiche*, in Aa.Vv. (a cura di), Liber amicorum *per Giuseppe Vettori*, Firenze, 2022, p. 1766 ss.

[38] All'art. 4, n. 4 del GDPR, l'attività di profilazione viene definita come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati 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». Importante, a questo proposito, il coordinamento con il DSA, che provvede a vietare quelle forme di *targeted advertising* realizzate mediante una profilazione dei fruitori dei servizi offerti dalle piattaforme online eseguite anche tramite l'utilizzo di quelle "categorie particolari di dati personali" contemplate all'art. 9, § 1, reg. UE 679/2016 (tra cui, appunto, "dati biometrici intesi a identificare

 ISBN 978-88-495-5568-4

del profitto, infatti, associando ai potenziali desideri e bisogni dell'utente pubblicità mirate di beni e servizi in grado di soddisfarli, tramite anche le facilitazioni offerte dall'intelligenza artificiale, è possibile massimizzare lo sfruttamento di ogni singolo dato raccolto dalle esperienze di navigazione degli utenti[39]. Ciò è reso possibile dal progressivo e inarrestabile diffondersi della c.d. *IoT* (*Internet of Things*), che tramite l'ausilio di potenti calcolatori, sistemi algoritmici, dispositivi intelligenti e una rete di sensori interconnessi, in grado di trattenere e processare un'imponente quantità di dati ricavati dalla navigazione degli utenti nell'infosfera[40], in un intervallo di tempo pressoché nullo, assicura lo svolgimento di attività statistiche e di catalogazione sempre più accurate al punto da poter predire, come detto, con elevato grado di approssimazione, i comportamenti individuali o di gruppi specifici di persone e financo orientare le abitudini degli stessi[41].

in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"); indicazioni in C. Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano,* in *Persona e mercato*, 2023, p. 40.

[39] La massimizzazione degli introiti di Google, principale *player* nel mercato del *targeted advertising*, ad esempio, conseguì proprio all'avanzamento tecnologico sul fronte dell'estrazione del c.d. *suprlus* comportamentale, regolamentato e protetto altresì dalla registrazione nel 2003 di un brevetto denominato *Generating User Information for Use in Targeted Advertising*. Sul punto S. Zuboff, *op. cit*., 87. Sui rapporti tra *targeted advertising* e intelligenza artificiale F. Galli, *La pubblicità mirata al tempo dell'intelligenza artificiale: quali regole a tutela dei consumatori?,* in *Contr. impr*., 2022, p. 919 ss.; V. Guggino e B. Banorri, *L'advertising ai tempi dell'intelligenza artificiale: algoritmi e marketing personalizzato*, in U. Ruffolo (a cura di), *Intelligenza artificiale: Il diritto, i diritti, l'etica*, Milano, 2020, p. 625 ss.

[40] Per una articolata rappresentazione dei caratteri di tale peculiare spazio virtuale L. Floridi, *Pensare l'infosfera. La filosofia come design concettuale*, Milano, 2020, p. 64 ss.; Id., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2007, p. 27 ss.

[41] Per una disamina dei molteplici profili connessi allo sviluppo dell'IoT v., in questo volume, M. Ziccardi, *Digitalizzazione*, cit.; nonché i diversi contributi raccolti in E. Gabrielli e U. Ruffolo (a cura di), *Intelligenza artificiale e diritto*, in *Giur. it*., 2019, c. 1657 ss.; G. Noto La Diega e I. Walden, *Contracting for the "Internet of Things": Looking into the Nest*, Queen Mary University, Legal Studies Research Paper, 219/2016, p. 1 ss.; J. Lima, *Insurers Look Beyond Connected Cars for IOT Driven Business Boom*, in *Computer Business Review*, 9 dicembre 2005, ove già si poneva in evidenza come «il vero valore dell'IOT dipende da come i clienti cambiano comportamenti e profili di rischio basandosi sul feedback ricevuto dalle loro "cose"». In questa direzione, ad esempio, importanti sono gli investimenti delle compagnie assicurative, le quali, pur essendo da tempo a conoscenza della correlazione tra rischio e personalità del conducente, non disponevano di strumenti adeguati (scil. sistemi senzienti di monitoraggio) per estrarre tali informazioni. La telematica moderna e i sistemi di *data mining*, potendo assicurare un flusso continuo di dati e sofisticate elaborazioni degli stessi, all'esito di integrazioni con i dati estratti da altri dispositivi (ad esempio gli smartphone), permettono agli assicuratori di poter monitorare e migliorare il comportamento dei propri assicurati, secondo un approccio chiamato "copertura del comportamento", attraverso la promozione di campagne promozionali "a premi" (con

ISBN 978-88-495-5568-4

La rielaborazione di tali informazioni che viene restituita all'utente, all'esito di una lettura esclusiva delle esperienze e delle informazioni così raccolte, però, non soltanto è condizionata dall'attendibilità dei dati processati e dalle capacità dell'algoritmo, ma appare fortemente manipolabile in quanto è sostanzialmente rimessa ai relativi programmatori la scelta dei parametri in ragione dei quali selezionare e ordinare i dati estratti e i contenuti digitali da proporre sulla base delle indagini predittive svolte[42].

Il capitalismo della terza modernità ha così ben presto mostrato il lato oscuro della rivoluzione digitale, palesando come a un avvio pieno di speranza circa la piena affermazione nello spazio digitale del diritto all'autodeterminazione di ciascuno[43], anche in ragione di un accesso all'informazione e a una moltitudine di servizi e contenuti digitali promosso come libero e (apparentemente) gratuito, corrispondesse un'incessante attività di raccolta ed estrazione di dati di navigazione, per un continuo riutilizzo degli stessi a fini commerciali per sfruttare, appunto, le munifiche opportunità provenienti dal *targeted advertising* e dall'«inquietante»[44] mondo del *neuromarketing*[45]. Forme aggressive di *advertising* quest'ultime che fondano i propri

sistemi *bonus* e *malus* che andranno evidentemente a incidere sul premio assicurativo), incentrate sulla disamina del comportamento alla guida degli utenti. Attraverso la definizione di una serie di parametri, ridotti in algoritmo – ad esempio, uso della cintura di sicurezza o dei segnalatori di direzione, velocità media, tempo di percorrenza dal punto di partenza a quello di arrivo, aggressività nelle accelerazioni e nelle frenate, numero di sorpassi o di km percossi oltre i limiti di velocità – si ritiene possa ottenersi una profilazione del conducente assai più precisa di quanto sia stato possibile fare per il tramite delle tradizionali variabili demografiche, così da ridurre incertezza e minimizzare il rischio. Sul punto cfr. gli studi di settore redatti da Aa.Vv. (a cura di), *Insurers Need to Plug into the Internet of Things-or Risk Falling Behind*, McKinsey, 8 gennaio 2017; Aa.Vv. (a cura di), *Overcoming Speed Bumps on the Road to Telematics*, Deloitte University Press, 21 aprile 2014; Aa.Vv. (a cura di), *The Internet of Things: Opportunity for Insurers*, ATKearney, 2014.

[42] Ulteriori indicazioni in proposito in G. Guzzardi, *Il paradigma identitario nella società digitale*, in *Persona e mercato*, 2023, p. 524 ss.

[43] Sull'affermazione del «diritto costituzionalmente garantito all'autodeterminazione consapevole in ogni ambito patrimoniale e non patrimoniale di ogni relazione fra privati» v. G. Vettori, *Il contratto senza numeri e aggettivi,* in *Persona e mercato*, 2012, p. 15; ampiamente in Id., *Contratto e rimedi*, Padova, 2017, p. 786 ss.

[44] G. Vettori, *Rodolfo Sacco e la civilistica del XXI secolo,* in *Riv. trim. dir. proc. civ*., 2023, p. 552, ove si evidenzia come, già in tempi non sospetti (R. Sacco, *Diritto muto. Neuroscienze*, *conoscenza tacita, valori condivisi*, Bologna, 2015), l'illustre A. avesse intuito le problematiche connesse al prepotente imporsi della data economy e allo sviluppo dei sistemi di IA, in ragione delle interrelazioni tra plurime questioni – come quelle inerenti al trattamento dei dati, alle (inquietanti) pratiche di *neuromarketing* e alla negoziabilità dei dati personali – che, pur ponendo tutte distinti ordini di problemi, appaiono parimenti centrali per una piena comprensione delle dinamiche dei mercati digitali.

[45] Estensione della neuro-economia, rivolta allo studio delle interrelazioni tra il processo decisionale umano e gli stimoli esterni a cui una persona può essere esposta avuto riguardo alla decisione di procedere all'acquisto di un bene o servizio. Sul punto, oltre alle

 ISBN 978-88-495-5568-4

paradigmi economici sulle risultanze della *behavioral Law & Economics* e sulla dimostrata capacità delle emozioni e delle propensioni psicologiche di influenzare la scelta del consumatore[46].

Una volta realizzato che i dati «più predittivi», ossia che generano maggiori profitti, sono quelli estratti all'esito di interventi mirati sui comportamenti degli utenti, i colossi del *web* non hanno esitato ad affinare ulteriormente le proprie strategie commerciali, non limitandosi più a *rilevare*, ma spingendosi addirittura a *formare* i comportamenti degli utenti in rete, attraverso l'utilizzo di sistemi predittivi alimentati proprio dalla (presunta) conoscenza acquisita in ordine a interessi, bisogni e persino stati d'animo degli utenti[47]. Ciò in osservanza di uno dei mantra del capitalismo della sorveglianza, secondo il quale un comportamento imprevedibile, spontaneo, non automatizzato dell'utente digitale «equivale a un guadagno perso»[48].

4. La rilevanza assunta dalle informazioni ricavabili dalle esperienze di navigazione degli utenti in rete – monitorabili e persino influenzabili, come

indicazioni fornite in questo volume nel citato contributo di E. Tuccari, v. M. Diotto, *Neurobranding. Il neuromarketing nell'advertising e nelle strategie di brand per i marketer*, Milano, 2020; P. Kotler, S. Hollensen e M. Opresnik, *Social media marketing, Marketer nella rivoluzione digitale*, Milano, 2019, p. 24 ss.; M. Lindstrom, *Neuromarketing. Attività cerebrale e comportamenti d'acquisto*, Milano, 2009; sui rischi connessi a «un'operazione di velamento», al punto da rendere invisibili le pratiche di *neuromarketing*, riscontrabile nella proposta di regolamento sull'IA, cfr. S. Orlando, *Regole di immissione*, cit., p. 366 ss.

[46] Ampiamente C.R. Sunstein, *Behavioral Law & Economics*, Cambridge, Cambridge University Press, 2000; C. Jolls, C.R. Sunstein e R.H. Thaler, *A Behavioral Approach to Law and Economics*, in *Standford Law Review*, 1998, p. 1471 ss. A questo proposito, divengono indicazioni preziose da convertire in surplus predittivo, ad esempio, le informazioni circa il proprio stato d'animo, fornite dall'utente stesso tramite il mero aggiornamento del proprio status sui social network o l'utilizzo di determinate *emoticon* nelle chat di messaggistica istantanea o, ancor più semplicemente, attraverso la stessa mimica facciale rilevabile da sempre più diffusi e sofisticati sistemi di riconoscimento biometrico. Approfondimenti in G. Guzzardi, *Il paradigma*, cit., 530 ss.

[47] S. Zuboff, *op. cit*., p. 18, ove si evidenzia, tra l'altro, come tali indagini predittive, provenienti dallo sfruttamento del surplus comportamentale, assumano enorme rilievo nel c.d. mercato dei comportamenti futuri. A questo proposito, a titolo esemplificativo, si pensi alla funzionalità *Driving Mode*, introdotta da Google nel 2016 per uno dei suoi prodotti di punta (*Google Maps*), in grado di suggerire destinazioni da esplorare o esercizi commerciali prima ancora che l'utente abbia selezionato dove voler andare o alle piattaforme di servizi musicali, film e prodotti di intrattenimento in grado di proporre all'utente, previa registrazione, contenuti digitali dedicati, rispetto ai quali non è affatto agevole comprendere se la preselezione sia stata effettuata sulla base di una effettiva profilazione dell'utente da parte dell'algoritmo che governa la piattaforma o se quest'ultimo, invece, così procedendo, promuova, in forma velata, messaggi, dottrine, stili di vita o, molto più semplicemente, determinati prodotti commerciali a scapito di altri, lasciando peraltro intendere che gli stessi risulterebbero quelli più popolari o più rispondenti agli interessi dell'utente.

[48] S. Zuboff, *op. cit*., p. 164.

ISBN 978-88-495-5568-4

detto, secondo logiche capitalistiche – richiama l'attenzione sulla effettiva allocazione e sulle relative modalità di circolazione della ricchezza nella *digital economy*, essendo non più trascurabile la riflessione circa la possibile configurabilità di prerogative proprietarie sui dati digitali e la conseguente capacità degli stessi – siano essi personali, pseudonimizzati, anonimizzati o semplici dati generici di navigazione – di acquisire autonomo valore di scambio.

Nella primavera del 2019 il Parlamento europeo e il Consiglio avviano una lunga (e ancora incompiuta) stagione di riforme per la regolamentazione del settore digitale, intervenendo, per quanto di interesse, in particolare, in tema di contratti di fornitura di contenuti e servizi digitali e di vendita di beni[49].

Trattasi di un mercato letteralmente dominato dai colossi statunitensi dell'ICT (*Information and Communication Technologies*), per cui non può certo trascurarsi la posizione di netta apertura della letteratura nordamericana[50], seppur con la dovuta attenzione alle significative differenze che intercorrono negli stessi ordinamenti continentali intorno al concetto di proprietà e, dunque, al fatto che la traduzione del termine "*ownership*" può dar luogo all'accostamento, in chiave comparativa, di istituti simili ma non per questo sovrapponibili[51].

Affermare, allora, che taluno possa essere nella disponibilità o titolato all'utilizzo ("*entitlement*") di dati (a maggior ragione se espressione della personalità del titolare) non equivale certo ad affermarne la titolarità esclusiva; allo stesso modo la circostanza che i dati digitali possano formare oggetto di un accordo avente contenuto patrimoniale non determina alcun passo indietro sul piano della tutela dei diritti, a patto di non perdere mai di vista la differente posizione gerarchica dei valori e degli interessi coinvolti[52]. Nello spazio digitale, secondo un autorevole orientamento, si assiste-

[49] Il riferimento è alle direttive (UE) nn. 770 e 771 del 17 aprile e del 20 maggio 2019, recepite in Italia, rispettivamente, con il d.lgs. 4 novembre 2021, n. 173, che ha determinato la novella del titolo III, parte IV del codice del consumo con l'aggiunta di un capo I-bis e, nel dettaglio degli artt. da 135-*octies* a 135-*vicies ter*, e con il decreto legislativo di pari data n. 170/2021, con cui è stato novellato il capo I del titolo III, parte IV del codice del consumo, contenente gli artt. da 128 a 135-*septies*.

[50] P.M. Schwartz, *Property, Privacy, and Personal Data*, in *Harvard Law Review*, 2004, p. 2055 ss.; V. Bergelson, *It's Personal But Is It Mine? Toward Property Rights in Personal Information*, in *UC Davis Law Review*, 2003, p. 379 ss.

[51] V. Zeno Zencovich, "*Do "Data markets" Exist?",* in *Medialaws*, 2019, 2, pp. 4-5.

[52] Sul punto, da ultimo, G. Guzzardi, *Il paradigma*, cit., p. 533 ss.; S. Troiano, *Il contratto tra analogico e digitale,* in *Pactum*, 2022, p. 56; C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, p. 57 ss. Sul tema della gerarchia dei valori, al cui vertice non può che esservi la persona, per tutti, P. Perlingieri, *La personalità umana nell'ordinamento giuridico*, Napoli-Camerino, 1972, ora in Id., *La persona e i suoi diritti*, Napoli, 2005, p. 5; nonché D. Messinetti, *Personalità (diritti della),* in *Enc. dir.,* XXXIII, Milano, 1983, p. 366 ss.; A. Nicolussi, *Autonomia privata e diritti della personalità,* in *Enc. dir., Annali*, IV, Milano, 2011, p. 133 ss.; G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 30 ss.

 ISBN 978-88-495-5568-4

rebbe all'affermazione di un "*license model*", piuttosto che del tradizionale paradigma della vendita, al quale non conseguirebbe alcun trasferimento a titolo definitivo di dati, bensì soltanto una concessione di utilizzo[53].

Il conflitto è tra due modelli antitetici, tra una visione patrimonialistica e una orientata in chiave personalistica[54]; il Garante europeo per la protezione dei dati personali, con il parere n. 4 del 17 marzo 2017, a tal proposito, ha inteso mettere in guardia da disposizioni legislative che potessero condurre a una valutazione in termini di liceità lo scambio di beni e servizi contro dati[55]. Riflessioni queste ultime che hanno senz'altro influenzato la stesura della versione definitiva della citata direttiva 2019/770 sui contratti di fornitura di contenuti e servizi digitali[56], se è vero che all'originaria esplicita equiparazione tra prezzo e dati nella definizione della controprestazione dell'utente, contenuta nella proposta di direttiva[57], abbia fatto seguito un più blando e generico riferimento al «caso» in cui, a fronte della fruizione di servizi digitali, l'utente si trovi a trasferire propri dati personali, evidentemente non in una condizione di sinallagmaticità[58].

Le ultime indicazioni in materia del legislatore unionale, tuttavia, sembrerebbero propendere per una visione più neutra dei dati digitali, se solo si consideri che, per la prima volta nel *Data Governance Act* (cfr. art. 2, § 1, n. 1) – ma la formulazione è parimenti ripresa tanto nel *Digital Markets*

[53] Così V. Zeno Zencovich, "*Do "Data markets"*, cit., p. 5.

[54] Per una panoramica sulle distinte posizioni al riguardo cfr. G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, p. 137 ss.

[55] Consultabile sul sito istituzionale dell'Autorità. Sul punto F. Bravo, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act,* in *Contr. impr./Eur*., 2021, p. 212; Id., *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto,* in *Contr. impr*., 2019, p. 34 ss. Nella giurisprudenza, Tar Lazio, 10 gennaio 2020, n. 260, in *Giur. it*., 2021, c. 320, con nota di C. Solinas, *Trattamento dei dati personali e pratiche commerciali scorrette*.

[56] Da ultimo indicazioni in I. Rapisarda, L*a privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche,* in *Nuove leggi civ. comm*., 2023, p. 203, nt. 61; S. Troiano, *op. cit*., p. 56, nota 37. Per approfondimenti sulla direttiva (UE)2019/770 v. 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, p. 507; A. De Franceschi, *La vendita di beni con elementi digitali*, Napoli, 2019, p. 13 ss.

[57] Nell'originaria Proposta di direttiva del 9 dicembre 2015, COM(2015)634 *final* 2015/0287 del Parlamento europeo e del Consiglio relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, si faceva espresso riferimento, infatti, ai «contratti in cui il fornitore fornisce contenuto digitale al consumatore, o si impegna a farlo, e in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato».

[58] Ampiamente C. Camardi, *op. cit*., p. 505 ss., la quale, peraltro, non manca di rilevare (alla successiva p. 507), che «la definizione poi abbandonata aveva un duplice pregio, quello di fotografare senza veli la realtà dei modelli commerciali praticati dai fornitori di servizi digitali, e quello di configurare coraggiosamente e di conseguenza un contratto di scambio tra servizi e dati personali, nell'ambito dei quali gli uni sono controprestazione degli altri».

ISBN 978-88-495-5568-4

Act (art. 2, § 1, n. 24) quanto nel *Data Act* (art. 2, § 1, n. 1) –, si provvede a definire, direi in maniera olistica almeno rispetto alle vicende proprie dello spazio digitale, i «dati» come "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva"[59].

L'indicazione è stata letta nei termini di un significativo spostamento del baricentro normativo a favore della *data economy* e di un netto *revirement* rispetto all'impostazione tradizionale di un sistema unipolare in cui assoluta primazia riveste la protezione (e il principio di minimizzazione del trattamento) dei dati personali, in ragione delle manifestate nuove esigenze di promozione dell'accesso, della disponibilità e della condivisione dei dati in funzione eminentemente concorrenziale[60]. Tuttavia, coerentemente con le previsioni inderogabili di legge, i valori e i principi generali che reggono le principali democrazie mondiali e, nello specifico, che vietano gli atti di disposizione del corpo che potrebbero determinare una lesione della dignità e irripetibilità dell'essere umano, ad avviso di chi scrive, dovrebbe ritenersi impedito all'utente poter negoziare quei dati digitali rappresentativi la propria esclusività e unicità e non paiono rinvenirsi indicazioni di segno contrario a tale assunto, nemmeno nelle ora richiamate novità legislative di rango unionale[61]. Ciò, sebbene, per un diverso avviso, proprio dall'assenza, in tema di trattamento dei dati personali, di disposizioni analoghe a quelle che, in tema di atti di disposizione di parti del corpo umano, espressamente vietano che gli stessi possano costituire fonte di lucro, deriverebbero, piuttosto, validi argomenti a sostegno della tesi secondo cui la monetizzazione dei dati personali non avrebbe nulla di disdicevole in sé nell'eventualità in

[59] Per un primo approfondimento sul reg. (UE)2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati (c.d. DGA) e sul successivo reg. (UE)2023/2854 del Parlamento Europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (c.d. DA), in questo volume, v. i contributi di G. Marino e G. Versaci; nonché, ampiamente, G. Resta, *Towards a unified regime of data-rights?*, in *Governance of/through big data*, a cura di G. Resta e V. Zeno Zencovich, Roma, 2023, p. 643 ss.

[60] Sul punto si rinvia al contributo di G. Marino, anche per ulteriori indicazioni bibliografiche in ordine a tale prospettiva metodologica.

[61] Sull'affermazione anche in termini di princìpi generali immanenti alle democrazie mondiali delle tutele e dei diritti attinenti alla persona (e, nello specifico, alla libertà di autodeterminazione e al consenso informato) v. G. Alpa, *I principi generali. Una lettura giusrealistica,* in *Giust. civ*., 2014, p. 962 ss., nell'àmbito di un'ampia indagine sul ruolo dei princìpi nell'ordinamento interno e in quello comunitario e sulle plurime funzioni (ordinante, direttiva, nomofilattica, armonizzante, integrativa) degli stessi; nella giurisprudenza, in particolare, Corte cost., 23 dicembre 2008, n. 438, in *Foro it*., 2009, 1, c. 1328. Sulla primazia dei valori e dei princìpi ancora G. Vettori, *Contratto giusto e rimedi effettivi,* in *Riv. trim. dir. proc. civ*., 2015, p. 788 e N. Irti, *La crisi della fattispecie,* in *Riv. dir. proc*., 2014, p. 38 ss., ove si evidenzia, in particolare, come i valori «valgono in sé e per sé, non hanno bisogno di altre norme o di tramiti, ma si appoggiano soltanto a sé stessi».

 ISBN 978-88-495-5568-4

cui fosse preceduta dall'acquisizione di un valido consenso, espressione di una «autodeterminazione informativa»[62].

La base della transazione "servizi contro dati" risulterebbe, quindi, pur sempre il consenso, con la conseguenza che, almeno riguardo ai rapporti intrattenuti nei mercati digitali tra una *data company* e una persona fisica – la quale assume (quantomeno in Europa) sempre la qualificazione di consumatore[63] – il riferimento non potrebbe che essere, prioritariamente, il reg. (UE) 679/2016[64]. L'art. 4, § 2, n. 11 del GDPR, a questo proposito, definisce il consenso un atto giuridicamente vincolante soltanto se espressione di una manifestazione di volontà "libera"[65]; forti perplessità al riguardo sussistono circa la considerazione di quella espressa rispetto ai c.d. *click wrap agreement* o, ancor prima, all'atto dell'"adesione ai termini di servizio o uso", quale effettiva condivisione di pratiche, prassi e condizioni[66].

L'utente digitale, normalmente interessato a concludere l'operazione negoziale nel più breve tempo possibile, con un gesto ormai divenuto pressoché automatico, "spunta" l'adesione alle condizioni del servizio senza particolarmente curarsi del relativo contenuto, e non certo perché già di sua conoscenza, bensì perché consapevole del fatto che la mancata accettazione delle condizioni esposte (e unilateralmente predisposte) impedirebbe di proseguire la navigazione e, quindi, di concludere l'affare. Il tempo di eventuale lettura, non a caso, è spesso inversamente proporzionale all'estensione di tali clausole, tanto che, nella letteratura nord-americana, si giunge a definire tale prassi come una vera e propria "umiliazione morale" della legge, nonché di un istituto cardine del diritto patrimoniale come l'accordo[67].

In tale percorso di svalutazione la digitalizzazione ha avuto un rilievo determinante. Anche soltanto in termini di costi, il cartaceo imponeva limiti naturali a termini di servizio ridonanti e prolissi; i contratti digitali, invece, sono "senza peso", con la conseguenza che, nonostante la loro

[62] Così, autorevolmente, G. Resta e V. Zeno Zencovich, *op. cit*., pp. 430-433.

[63] V. Zeno Zencovich, "*Do "Data markets"*, cit., p. 13.

[64] Nella stessa dir. (UE)770/2019, all'art. 3, § 8, in attuazione del considerando 37, si riconosce la preminenza delle regole del GDPR, disponendo che, «in caso di conflitto tra le disposizioni della presente direttiva e del diritto dell'Unione in materia di protezione dei dati personali, prevale quest'ultimo». Ampi riferimenti alla portata regolativa e alle finalità del GDPR in questo volume nel contributo di M. Renna, *L'identità sicura: il banco di prova del data breach*.

[65] Da ultimo, riferimenti in I. Rapisarda, *La* privacy *sanitaria*, cit., p. 200 ss.

[66] Tutto ciò non senza considerare come, ai sensi del successivo art. 6, alla morte dell'interessato, cesserebbe l'efficacia autorizzativa del consenso, difettando, in assenza di specifiche disposizioni sul punto, un'idonea base del trattamento dei dati dell'utente digitale deceduto; sul punto G. Marino, *op. cit*., p. 212.

[67] M.J. Radin, *Boilerplate: The fine print. Vanishing right, and the Rule of Law*, Princeton, Princeton University Press, 2012, p. 16 ss.

ISBN 978-88-495-5568-4

particolare "voluminosità", possono essere proposti al cliente e archiviati senza particolari costi supplementari.

In questo contesto – e una solida conferma la si rinviene all'art. 7, comma 4, del GDPR – non appare potersi ritenere libera (e informata) la concessione del consenso all'utilizzo dei dati personali, ogni qualvolta richiesti, attraverso l'obbligatoria registrazione e creazione di *account*, per la fruizione di contenuti digitali, sebbene indicazioni in tal senso sembrerebbero provenire da autorevole dottrina[68], la quale, in precedenza, non aveva comunque mancato di osservare come i dati personali non possano essere trattati come merci e un consenso «remunerato» sarebbe, per definizione, «non libero»[69].

L'equiparazione dello schema "servizi contro dati" a quello "servizi contro prezzo", peraltro, imporrebbe di riconsiderare le stesse modalità di fruizione e accesso ai servizi digitali da parte degli utenti; laddove si intendesse instaurata una vera e propria relazione contrattuale, in osservanza dei precipui obblighi di buona fede e correttezza gravanti sulle parti contrattuali, anche l'utente non potrebbe che ritenersi soggetto all'obbligo di veridicità e, nello specifico, di esattezza dei dati personali trasmessi[70]. La prospettazione dello schema "servizi contro dati" nei termini di una compiuta dinamica contrattuale, ancora, contrasterebbe con la stessa previsione dell'art. 7 del GDPR che dispone la revocabilità del consenso al trattamento dei dati personali "in qualsiasi momento", atteso che l'esercizio del diritto di revoca all'uso dei dati, nell'economia del rapporto contrattuale, determinerebbe un effetto simile a quello di un recesso unilaterale, di certo, non sempre consentito in una relazione tipicamente contrattuale[71].

Potrebbe avanzarsi l'idea che, essendo coinvolte sfere di intangibilità della persona umana, il noto principio *pacta sunt servanda* che governa la materia contrattuale incontrerebbe una significativa deroga, ma la stessa valorizzazione di tale eccezione non avrebbe l'effetto di confermare la validità della regola, piuttosto risulterebbe un significativo argomento per

[68] G. Resta e V. Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete,* in *Riv. trim. dir. proc. civ*., 2018, p. 430.

[69] G. Resta, *Doni non patrimoniali*, in *Enc. dir., Annali*, IV, Milano, 2011, p. 510 ss. Sul punto, più di recente, anche il considerando 24 dir. (UE)770/2019, il quale, esplicitamente, declama che «la protezione dei dati personali è un diritto fondamentale e che tali dati non possono dunque essere considerati una merce».

[70] In questa direzione non si sottovaluti la previsione nelle condizioni generali di Facebook o Amazon dell'obbligo per l'utente di fornire dati anagrafici esatti e aggiornati, nonché di comunicare tempestivamente ogni eventuale variazione.

[71] P. Perlingieri, P*rivacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap*., 2018, p. 484; G. Resta, *Autonomia privata,* cit., p. 123; più di recente G. Versaci, *op. cit*., p. 182 ss. In termini generali sulla revoca del consenso al trattamento dei dati G. Resta, *Revoca del consenso e interesse al trattamento nella legge sulla protezione dei dati personali,* in *Riv. crit. dir. priv*., 2000, pp. 327-333.

 ISBN 978-88-495-5568-4

confutarla[72]. Pur risultando ammissibile, nell'ottica di un bilanciamento tra valori, al passo con il mutare delle dinamiche sociali, una limitata negoziabilità di diritti della personalità, ciò non appare possibile nel caso in cui siano coinvolti valori intrinseci, non rinunziabili, della persona umana e attinenti alla rappresentazione della persona nella vita di relazione e nella realtà sociale, aggiungeremmo oggi, a prescindere se concretizzatasi in uno spazio fisico o virtuale[73].

Nelle logiche dell'economia digitale, evidentemente non sempre sorrette da sano antropocentrismo, anche in ragione di una vera e propria «dittatura dell'algoritmo»[74], emblema della società della spersonalizzazione, l'utente assume rilievo non per il valore intrinseco e irripetibile della persona umana, quanto piuttosto per l'indistinta capacità di trasferire dati ed esperienze – beni non rivali –, quali fonti inesauribili di informazioni riutilizzabili e, dunque, continuamente monetizzabili[75]. In una sorta di un nuovo "umanesimo digitale", allora, occorre identificare le condizioni etiche per uno sviluppo delle nuove tecnologie che valorizzi e non rinunci ai tratti caratterizzanti della nostra umanità, nella consapevolezza che è l'uomo a creare (e, dunque, a governare) la tecnologia e non il contrario[76].

Ogni mercato, secondo le proprie logiche di profitto, è votato a invadere ambiti di esclusiva pertinenza di utenti e fruitori, ma anche al cospetto

[72] Sull'articolata relazione tra regole e principi, di recente, G. Vettori, *La funzione del diritto privato in Europa*, in *Persona e mercato*, 2018, p. 149 ss.; Id., *Regole e principi. Un decalogo,* in *Nuova giur. civ. comm*., 2016, p. 124 ss.; in precedenza, per tutti, L. Mengoni, *Diritto e tecnica*, 2001, ora in Id., *Scritti, Metodo e teoria giuridica*, Milano, I, 2011, p. 47; Id., *I Principi generali del diritto e la scienza giuridica*, in *I principi generali del diritto*, Roma, 1992, p. 317 ss.

[73] Per un equilibrato bilanciamento tra diritti e libertà fondamentali – nel caso di specie, tra la dignità della persona umana e la libertà di prestazione di servizi e la circolazione delle merci – e l'affermazione, proprio per il tramite di un prudente richiamo ai principi generali, della primazia dei diritti della personalità, costituiscono un valido punto di riferimento le argomentazioni di Corte giust., 14 ottobre 2004, c. 36/02, *Omega*, in *Corr. giur*., 2005, p. 486 ss., con nota di R. Conti, *La dignità umana dinanzi alla Corte di Giustizia* e di E. Pellecchia, *Il caso Omega: la dignità umana e il delicato rapporto tra diritti fondamentali e libertà (economiche) fondamentali nel diritto comunitario,* in *Eur. dir. priv*., 2007, p. 181 ss.; già Cass., 22 giugno 1985, n. 3769, in Foro it., 1985, I, c. 2211, sul noto "*caso Veronesi*".

[74] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014, p. 37.

[75] Sul punto ancora G. Guzzardi, *Il paradigma*, cit., p. 536 ss.; ulteriori indicazioni in E. Morozov, *Silicon Valley: i signori del silicio*, trad. a cura di F. Chiusi e T. Albanese, Torino, 2017, p. 21, il quale, senza mezzi termini, descrive le piattaforme come parassiti, che si nutrono delle relazioni sociali ed economiche esistenti e al cui strapotere urge porre rimedio.

[76] Sul punto v. l'indagine sociologica di D. Cardon, *Che cosa sognano gli algoritmi. Le nostre vite al tempo dei big data*, tra. it. a cura di C. De Carolis, Milano, 2016, p. 1, secondo il quale l'algoritmo «organizza gerarchicamente l'informazione, indovina ciò che ci interessa, seleziona i beni che preferiamo e si sforza di sostituirci in numerosi compiti. Siamo noi a fabbricare questi calcolatori, ma in cambio loro ci costruiscono».

ISBN 978-88-495-5568-4

di nuove tecnologie che puntano con decisione a proiettare l'uomo in una dimensione ulteriore e virtuale (pronta persino a propagarsi nel metaverso)[77] – al punto da registrare, come detto, l'ambizione dei capitalisti della sorveglianza a uno spazio digitale senza regole[78] –, il diritto non può abdicare alla propria funzione ordinante e regolatrice[79]. Le peculiari caratteristiche e l'effettiva assenza di confini del mercato digitale senz'altro rendono evidente la scarsa adattabilità delle norme statuali, ma in alcun modo potrebbero giustificare la rappresentazione di tale spazio nei termini di una zona franca in cui dovrebbe persino tollerarsi – quasi nei termini di una "inevitabile" conseguenza – una riduzione delle tutele normalmente assicurate, in un contesto analogico, a qualsiasi relazione interindividuale (sia essa il frutto dell'esercizio dell'autonomia privata personale o patrimoniale)[80], dovendosi ritenere la stessa, prima di tutto, soggetta al governo di quelle categorie e alla carica assiologica di quei princìpi comuni alle democrazie mondiali e che assistono il giurista nella comprensione e nella decodificazione dei fenomeni sociali[81].

[77] Per un primo inquadramento dei diritti degli utenti nel metaverso v. F. Sarzana Di Sant'Ippolito, *Il diritto del metaverso. NFT, Defi, Gamefi e Privacy*, Torino, 2022; da ultimo R. Bocchini, *Nuovi beni digitali e mondi dematerializzati. Il metaverso,* in *Eur. J. Privacy Law & Tech*., 2023, p. 45 ss.

[78] Sull'invocata *net-neutrality* da parte dei tech giants si rinvia alle indicazioni bibliografiche fornite alla nota 3.

[79] Sulla funzione ordinante del diritto G. Vettori, *Regole e principi*, cit., p. 124 ss. e, nello specifico, dei princìpi v. G. Alpa, *op. ult. cit*., p. 961; G. Oppo, *Princìpi*, in *Tratt. dir. comm. Buonocore*, I, 1, Torino, 2001, p. 12 ss. Sui riflessi delle innovazioni tecnologiche sui rapporti sociali e le libertà fondamentali, nonché sul ruolo del legislatore al tempo della data economy, da ultimo, S. Orlando, *Per un sindacato*, cit., p. 530 ss.

[80] Per un approfondimento sulle distinte forme di articolazione dell'autonomia privata, di recente, G. Di Rosa, *Il contratto. Appunti di parte generale*, Torino, 2021, p. 8 ss.

[81] Princìpi e valori universali a cui, in ogni caso, è assicurata una tutela multilivello, guidando, ovviamente, anche le scelte legislative di fondo degli ordinamenti continentali; alle disposizioni in merito della Carta costituzionale (segnatamente, gli artt. 1-12 e 41 Cost.) e della Dichiarazione Universale dei Diritti dell'Uomo, adottata dalle Nazioni Unite il 10 dicembre del 1948, si aggiungano, ad esempio, quelle contenute nella Carta dei diritti fondamentali dell'UE (2000/C 364/01, ma in vigore dal 1° dicembre 2009 con il Trattato di Lisbona) o già nella Convenzione di Oviedo per la protezione dei diritti dell'uomo nell'applicazione della biomedicina, la quale, con un omnicomprensivo riferimento alla scienza, all'art 1, indica quale sua finalità la protezione dell'essere umano «nella sua dignità e nella sua identità». Per tutti, G. Alpa, *op. ult. cit*., p. 957 ss.; P. Perlingieri, *Il diritto civile nella legalità costituzionale*, Napoli, 2006, p. 416 ss.

 ISBN 978-88-495-5568-4

Emanuele Tuccari

Note minime sull'asistematica disciplina del *neuromarketing*

Sommario: 1. Introduzione. – 2. Il problema del *neuromarketing*. – 3. L'assenza di una disciplina sistematica e le prime risposte dell'ordinamento. - 3.1. Il trattamento dei dati biometrici: la disciplina del GDPR. - 3.2. Il rischio di un abuso del *neuromarketing* e la minaccia al libero arbitrio dell'individuo. - 3.2.1. Una pratica commerciale sleale? Con che rimedi privatistici? - 3.2.2. La più recente normativa dell'Unione Europea: l'AI Act. - 4. Un difficile coordinamento? Il caso del *Digital Services Act.* – 5. Considerazioni conclusive.

1. Già nel 1961, un grande Maestro del diritto civile come Michele Giorgianni (percepiva e) denunciava il rischio di "affrontare situazioni nuove con strumenti vecchi"[1]. Quest'avvertimento, meritevole della massima attenzione anche da parte dell'odierno interprete, risulta di stringente attualità a fronte dell'inarrestabile evoluzione (*in primis*, tecnologica) destinata a trasformare celermente ampi settori della società contemporanea.

L'intero mondo del *marketing* non fa, di certo, eccezione. Un mondo che, sempre più, si caratterizza non soltanto per l'assunzione di diversi caratteri delle (vecchie e nuove) forme di pubblicità commerciale rivolta ai consumatori, ma anche per l'ampliamento dello spettro delle varie finalità perseguite, affiancandone, con il passare del tempo, di nuove a quelle, più tradizionali, di matrice prettamente commerciale. Il *marketing*, secondo la letteratura di settore, costituisce, infatti, l'insieme di procedure e tecniche che sono studiate, elaborate, testate, messe in opera, controllate, adattate e modificate continuamente da funzioni interne alle organizzazioni che se ne

[1] M. Giorgianni, *Il diritto privato ed i suoi attuali confini ("prolusione" accademica letta a Napoli nel 1961),* ora *in Le prolusioni dei civilisti*, III, (1940-1979), Napoli, 2012, p. 2943 ss., spec. p. 2946. L'*incipit* appare calzante non soltanto per evidenti ragioni di merito (che si spera di far apprezzar al lettore anche nel prosieguo della trattazione), ma anche perché l'Autore risulta decisamente legato all'ateneo catanese come a quello pavese, avendo lasciato un'impronta, per un verso, proprio a Catania (città "accademicamente" natale, dove frequentò il corso del suo Maestro, Rosario Nicolò, e conseguì la cattedra universitaria, prima di proseguire la sua attività presso l'Università di Bologna, di Napoli e, infine, di Roma "La Sapienza") e, per un altro verso (seppure decisamente minore), anche a Pavia, dove fu uno dei redattori del pre-progetto di Code éuropeen des contrats allestito dalla commissione presieduta dal prof. Giuseppe Gandolfi presso l'Accademia dei Giusprivatisti Europei (ancor oggi collocata presso il Dipartimento di Scienze Politiche e Sociali dell'Università di Pavia).

 ISBN 978-88-495-5568-4

avvalgono, o da società esterne alle quali queste funzioni sono affidate in tutto o in parte, al fine di creare le più varie forme di comunicazione rivolte a categorie di destinatari, per sollecitare precise risposte comportamentali[2].

Oggi chi fa *marketing* disegna pertanto le proprie strategie su stili di vita, abitudini e credenze (storiche, religiose, politiche) delle persone, in quanto indirettamente funzionali al comportamento che si vuole influenzare, alla risposta che si vuole ottenere: un imprenditore commerciale mira a finalizzare un acquisto, un candidato politico desidera conseguire un voto, una chiesa aspira ad acquisire un nuovo membro nella propria comunità, etc. Ciascuno – tramite un'attività (più o meno complessa) di *marketing* – ricerca pertanto l'adesione a una determinata causa per ottenere uno specifico risultato[3].

Così – com'è stato, ormai da più parti, rilevato – il *marketing* presuppone, più generalmente, la preparazione del terreno affinché le successive sollecitazioni comportamentali abbiano successo. L'attività svolta dai *marketer* sulle credenze, sugli stili e sui comportamenti di vita delle persone è praticata in quanto ritenuta strategica, prodromica e strumentale rispetto all'influenza sulle specifiche risposte che si intendono ottenere. Nell'era dell'informazione digitale e dei *social media*, i *marketer* devono comprendere i comportamenti e alimentare lo stimolo all'*engagement* delle persone, facendosi trovare, all'esito di un'operosa e paziente attesa, pronti a cogliere tutte le opportunità messe a disposizione da un determinato mercato[4].

La presente riflessione non ambisce certamente ad affrontare in modo esauriente le molteplici problematiche sollevate dall'articolata (e già molto, forse perfino troppo, complessa) disciplina del polimorfo fenomeno del *marketing*, ma, più modestamente, mira ad evidenziare come l'evoluzione delle nuove tecnologie rilanci sfide classiche affiancandone di ulteriori – di carattere non soltanto economico, ma anche giuridico – a seguito della diffusione del c.d. "neuromarketing". S'intende pertanto soffermarsi sull'esigenza di un dialogo, divenuto improcrastinabile, fra neuroscienze, diritto ed economia per analizzare un fenomeno in espansione che – secon-

[2] Sul punto, cfr., per tutti, Ph. Kotler, K.L. Keller, A. Chernev, F. Ancarani e M. Costabile, *Marketing management*, 16ª ed., Milano, 2022, p. 26 ss., p. 32.

[3] Cfr., Ph. Kotler, *Marketing 4.0. Dal tradizionale al digitale*, Milano, 2017, p. 7 ss.; Ph. Kotler, S. Hollensen e M.O. Opresnik, *Social media marketing. Marketer nella rivoluzione digitale*, Milano, 2019, XVI ss., p. 2 ss.

[4] Tali profili sono già sottolineati nella panoramica sull'evoluzione del *marketing* (con una particolare attenzione ai possibili riflessi giuridici) di S. Orlando, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, in *Persona e mercato*, 2022, spec. p. 358; Id., *Per un sindacato di liceità del consenso privacy*, *ibidem*, 2022, pp. 532-533. Nella letteratura di settore, invece, v. Ph. Kotler, K.L. Keller, A. Chernev, F. Ancarani e M. Costabile, *Marketing management*, cit., p. 8 ss.

ISBN 978-88-495-5568-4

do l'insegnamento (anche) di Michele Giorgianni – dev'essere, per quanto possibile, governato con attenzione storica e prospettica.

2. Non è possibile neanche cominciar a riflettere sulla possibile disciplina del c.d. "neuromarketing" senza avere prima delineato, seppure sinteticamente, le fondamentali caratteristiche del fenomeno.

Il c.d. "neuromarketing" fa ricorso alle neuroscienze per applicazioni di *marketing*, offrendo così la possibilità di osservare direttamente pensieri, impressioni ed emozioni dei consumatori[5]. Secondo la *Neuromarketing Science and Business Association* (*NMSBA*, cioè la più famosa associazione internazionale di operatori), «Neuromarketing uses neuroscience to reveal subconscious consumer decision-making processes. Neuromarketers study brain and biometric responses, as well as behavior, to understand and shape how consumers feel, think, and act»[6]. Il *neuromarketing* costituisce pertanto «the application of measurement of physiological and neural signals in the field of marketing and it aims to understand unconscious reactions to marketing stimuli in order to provide insights into consumers' decision-making processes and to better predict purchasing behaviour»[7].

Nell'ambito del *neuromarketing* – acquisiti, e prontamente riadattati soprattutto a beneficio dell'interesse dei grandi operatori economici digitali, gli approdi fondamentali della c.d. "*behavioral Law & Economics*" (relativi, cioè, allo studio dei fattori psicologici, cognitivi, emotivi, culturali e sociali coinvolti nelle decisioni degli individui o delle istituzioni nonché di come queste decisioni finiscano per discostarsi, in realtà, da quelle impli-

[5] Cfr., per tutti, Z. Sethna, J. Blythe, *Consumer behaviour*, SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne, IV ed., 2019, pp. 25-26.

[6] La definizione è tratta direttamente dal sito della *Neuromarketing Science and Business Association, https://www.nmsba.com/neuromarketing/what-isneuromarketing*.

[7] Questa la definizione contenuta nel recente studio della Commissione Europea, *State of the art of neuromarketing and its ethical implications*, 2023, 7 (reperibile online all'indirizzo: *https://op.europa.eu/en/publication-detail/-/publication/43754ac8-26aa-11ee-a2d3-01aa75ed71a1/language-en*). Nello stesso senso, v. T.L. Tuten, *Principles of Marketing for a Digital Age*, SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne, 2020, pp. 140-141; M. Nilashi, S. Samad, N. Ahmadi, A. Ahani, R.A. Abumalloh, S. Asadi, R. Abdullah, O. Ibrahim e E. Yadegaridehkordi, *Neuromarketing: a review of research and implications for marketing*, in *Journal of Soft Computing and Decision Support Systems*, 2020, 7(2), p. 23 ss.; E. Bakardjieva e A.J. Kimmel, *Neuromarketing research practices: attitudes, ethics, and behavioral intentions*, in *Ethics & Behavior*, 2017, 27(3), p. 179 ss.; C.M.L. Cruz, J.F.D. Medeiros, L.C.R. Hermes, A. Marcon e É. Marcon, *Neuromarketing and the advances in the consumer behaviour studies: a systematic review of the literature*, in *International Journal of Business and Globalisation*, 2016, 17(3), p. 330 ss.; C. Morin, *Neuromarketing: The New Science of Consumer Behavior*, in *Society*, 2011, p. 131 ss.; N. Lee, A.J. Broderick e L. Chamberlain, *What is 'neuromarketing'? A discussion and agenda for future research*, in *International journal of psychophysiology*, 2007, 63(2), p. 199 ss.

 ISBN 978-88-495-5568-4

cite nella teoria economica classica e in quella giuseconomica)[8] – si ricorre pertanto a tecniche rivolte a compiere misurazioni fisiologiche. Si pensi, per esempio, all'elettroencefalogramma (*electroencephalography*, EEG), per misurare l'attività elettrica cerebrale, all'*eye-tracking*, per misurare i movimenti degli occhi e lo sguardo, alla risonanza magnetica funzionale (*functional magnetic resonance imaging*, fMRI), per rilevare quali aree del cervello si attivano durante l'esecuzione di determinati compiti, alla valutazione della risposta galvanica della pelle (*galvanik skin response*, *GSR*), per misurare le variazioni nelle caratteristiche elettriche della pelle in risposta ai cambiamenti degli stati emotivi, alle misure implicite ("*implicit measures*"), che misurano i tempi di risposta impiegati dal cervello per pensare, e, più genericamente, alla biometria, per studiare le risposte emotive e fisiche non intenzionali delle persone a sollecitazioni esterne (come la sudorazione, la respirazione, il battito cardiaco), nonché ai diversi altri sistemi di intelligenza artificiale per costruire, anche sulla base dei dati tratti dalle tecniche di cui sopra, modelli di simulazione e predittivi sulle risposte delle persone al *marketing*, ai prodotti, ai marchi e alle esperienze di acquisto.

Non appare più possibile pertanto trascurare la sempre più diffusa prassi e l'ormai sterminata letteratura specialistica – riconducibile, in particolare (ma non solo), alle neuroscienze, alla psicologia, alle scienze azienda-

[8] Il padre dell'economia comportamentale moderna è solitamente considerato lo psicologo israelo-statunitense Daniel Kahneman (recentemente scomparso). Nel 2002 ha ricevuto il premio Nobel per l'economia, per aver dimostrato, attraverso i suoi studi (condotti spesso con Amos Tversky), che le persone non prendono decisioni solo seguendo i propri interessi personali, ma che, invece, agiscono anche senza seguire criteri logici, saltando velocemente a conclusioni sbagliate e arrivando persino a pensare che eventi poco plausibili abbiano probabilità concrete di verificarsi. Cfr., *ex multis*, A. Tversky, D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases*, in *Science*, 1974, pp. 1124; D. Kahneman, A. Tversky, *«Prospect Theory»: An Analysis of Decision under Risk*, in *Econometrica*, 1979, p. 263 ss.; D. Kahneman, *Thinking, Fast and Slow*, London, 2011 (trad. it., Pensieri lenti e veloci, Milano, 2012). Nel corso del tempo, l'economia comportamentale è stata declinata, con grande successo, anche con riferimento alle decisioni microeconomiche e alle politiche pubbliche (v. R. Thaler e C.R. Sunstein, *Nudge. Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008, trad. it., *La spinta gentile. La nuova nuova strategia per migliorare le nostre decisioni su denaro, salute, felicità*, Milano, 2009; Richard Thaler è stato, a sua volta, premio Nobel per l'economia nel 2017). Per ulteriori approfondimenti, cfr. C.R. Sunstein, *Effetto nudge. La politica del paternalismo libertario*, Milano, 2015; C.R. Sunstein, *Behavioral Law & Economics*, Cambridge, (rist.) 2007; C. Jolls, C.R. Sunstein e R. Thaler, *A Behavioral Approach to Law and Economics*, in Standford Law Review, 1998, 50, p. 1471 ss. In Italia, v. M. Motterlini, *Economia emotiva*, Milano, 2008; Id., *Trappole mentali*, Milano, 2010. Nell'ambito della letteratura giuridica, si è soffermato sulla c.d. "*behavioral Law & Economics*" V. Roppo ("*Behavioural Law and Economics*", *regolazione del mercato e sistema dei contratti*, in *Riv. dir. priv*., 2013, p. 167 ss.) e, più di recente, per affrontare specificamente le problematiche poste dal *neuromarketing*, E.M. Incutti, (*Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale*, in *Giust. civ*., 2022, p. 520 ss.).

ISBN 978-88-495-5568-4

listiche ed informatiche[9] – che evidenziano la vitalità del *neuromarketing*, l'enorme valore economico degli investimenti in questo campo e, quindi, l'impatto significativo che tale realtà è destinata a produrre sulle vite delle persone negli anni a venire. Un ambito considerato relativamente nuovo fino a poco tempo fa, principalmente a causa delle barriere tecnologiche, della possibilità di trasformare i risultati delle neuroscienze in *insight* commerciali utili e degli alti costi di raccolta dei dati. L'evoluzione tecnologica costante sta rendendo però velocemente il *neuromarketing* uno strumento diffuso per il *customer insight*: una prospettiva non sempre facile da comprendere, ma soprattutto difficile da governare giuridicamente. Il *neuromarketing* risulta, infatti, un fenomeno tanto, per alcuni aspetti, affascinante quanto, per altri, inquietante, ponendo problemi e sfide per l'etica e per il diritto riconducibili a vecchi e nuovi rischi, derivanti da pratiche potenzialmente sempre più profittevoli per le aziende e pericolose per gli utenti[10]. Secondo la stessa Commissione europea, infatti, "*the rapid development of research methodologies and tools that can be used to record, understand and potentially alter human decision-making raises important ethical challenges*"[11]. Il ricorso ai suddetti strumenti di *neuromarketing* – fermo restando il ruolo (da sempre) centrale svolto dallo sviluppo tecnologico nel perseguimento d'interessi commerciali – non può che sollevare problematiche, a dir poco, rilevanti per il giurista, chiamato a comprendere ammissibilità, limiti e possibile disciplina di pratiche così invasive (giacché caratterizzate dall'osservazione diretta del funzionamento del corpo umano) e potenzialmente pericolose (poiché rivolte a decifrare ed influenzare, ove non addirittura manipolare, volontà e comportamento delle persone).

3. Alle sfide (vecchie e nuove) poste dal *neuromarketing* l'ordinamento "multilivello" (italiano ed eurounitario), in assenza di una specifica normativa, sembra ancor oggi rispondere in ordine sparso, suggerendo di ripercorrere l'evoluzione della normativa sulla profilazione e sul trattamento

[9] Il *neuromarketing* viene considerato pertanto come un "*growing research field*", con una "*multidisciplinary nature that integrates the approaches of neuroscience, psychology, and marketing, but also behavioural economics, decision-making theories, and computational analysis*" (European Commission, *State of the art of neuromarketing and its ethical implications*, cit., 7-8). Nello stesso senso, v. C.M.L. Cruz, J.F.D. Medeiros, L.C.R. Hermes, A. Marcon e É. Marcon, *Neuromarketing and the advances in the consumer behaviour studies: a systematic review of the literature*, cit., p. 330 ss.

[10] Per un'analisi critica, di stampo prevalentemente sociologico, con riferimento alle sempre più diffuse forme di condizionamento fortemente invasive, sebbene silenziose, compiute a beneficio degli interessi commerciali degli operatori del settore, v., per tutti, S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, pp. 269 ss., 297 ss.

[11] European Commission, *State of the art of neuromarketing and its ethical implications*, cit., p. 9.

 ISBN 978-88-495-5568-4

dei dati biometrici (§ 3.1.) e sull'eventuale minaccia al libero arbitrio della persona (consumatore e non solo) (§§ 3.2.; 3.2.1; 3.2.2).

Solo così sarà poi possibile proporre delle prime notazioni critiche, di carattere prevalentemente sistematico, anche alla luce dei difetti di coordinamento finora emersi fra le diverse normative (§§ 4 e 5).

3.1. Già dalla definizione stessa di "neuromarketing" emerge l'esigenza di riflettere sul fenomeno (ormai piuttosto noto nel contesto digitale) della profilazione (ovverosia, secondo l'art. 4, n. 4, del GDPR, di "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"). Tale fenomeno – preso in espresso esame anche nei considerando 24, 60, 63, 70, 71, 72, 73 e 91 nonché negli artt. 13 § 2, lett. f), 14, § 2, lett. g), 15, § 1, lett. h), 21, 22, 35, § 3, lett. a), 47, § 2, lett. e), 70, § 1, lett. f) del GDPR – si caratterizza, infatti, per un'articolata disciplina a tutela dell'interessato (a partire dall'esigenza di un'adeguata informazione con riferimento al fatto che i suoi dati verranno trattati a fini di attività promozionale e commerciale e che i suoi dati potranno essere comunicati a terzi, per poi passare al riconoscimento di un ampio diritto di opposizione e alla configurazione di una serie di rilevanti misure di garanzia). A ciò si aggiunge, nel caso di specie, la necessità di sviluppare una riflessione attenta anche al trattamento di categorie particolari di dati e, in particolare, di "dati biometrici". Questi, come noto, sono "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici" (art. 4, n. 14, GDPR)[12].

Mentre la definizione di dati biometrici risulta oggi piuttosto consolidata, le maggiori problematiche (interpretative e applicative) sembrano riguardare, invece, la disciplina relativa al trattamento dei dati biometrici, a cominciare proprio da quella dettata dal Regolamento UE 679/2016.

Si tratta, in particolare, di prender in considerazione le tutele specificamente previste con riferimento al trattamento delle categorie particolari di dati, cui si ascrivono, fra gli altri, i suddetti dati biometrici[13].

[12] Da ultimo, la definizione è stata peraltro ripresa dall'art. 3, n. 34, dell'AI Act ("'*biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, such as facial images or dactyloscopic data*").

[13] Cfr., *ex multis*, C. Jasserand, *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*, in *European Data Protection Law Review*, 2016, p. 297 ss.; E.J.

ISBN 978-88-495-5568-4

Nell'ottica di un'analisi – seppure necessariamente sintetica – di carattere sistematico, non è possibile trascurare la centralità del consenso dell'interessato. È lo stesso art. 9 del GDPR, infatti, a sottolineare – dopo aver imposto un divieto generale relativo al trattamento (delle categorie particolari di dati e) dei dati biometrici intesi ad identificare in modo univoco una persona fisica (§ 1) – la liceità del trattamento di tali dati personali se l'interessato ha prestato il proprio consenso esplicito per una o più finalità specifiche (§ 2, lett. a)[14].

Kindt, *An introduction into the use of biometric technology. Privacy and data protection issues of biometric applications: A comparative legal analysis*, Berlin, 2013, p. 12 ss.

[14] Come noto, sono previste solo alcune tassative eccezioni al divieto generale di trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché di trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, § 1, GDPR): "a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica

 ISBN 978-88-495-5568-4

Ne deriva l'ennesima occasione di riflessione – da inserirsi in un recente, ma già piuttosto ampio, dibattito dottrinale – sulla natura stessa del consenso dell'interessato[15], stavolta più specificamente declinato nell'articolata prospettiva del trattamento dei dati biometrici funzionali allo svolgimento di finalità di *marketing* nell'odierno contesto digitale.

Alla tradizionale visione del consenso "autorizzatorio" (formulata in origine specie a partire dalla lettura che, facendo leva sull'indisponibilità dei diritti della personalità, considera il consenso come lo strumento funzionale a rendere lecita un'attività, quale il trattamento dei dati, altrimenti illecita) sembra così lentamente affiancarsi una diversa visione (più negoziale) del consenso dell'interessato, che, impegnando quest'ultimo nei confronti del titolare, può essere anch'essa (forse perfino più facilmente) connessa, specie con riferimento alle categorie particolari di dati, alla specifica finalità perseguita (proprio ai sensi del suddetto art. 9, § 2, lett. a), GDPR)[16].

Tuttavia, le problematiche relative al trattamento dei dati biometrici non

o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato" (art. 9, § 2, GDPR).

Il trattamento in oggetto – con finalità di *neuromarketing* – non sembra poter rientrare pertanto in nessuna delle suddette eccezioni, se non in astratto sub art. 9, § 2, lett. a), in presenza di un esplicito consenso dell'interessato al trattamento di tali categorie particolari di dati personali per una o più finalità specifiche.

[15] Per una panoramica sull'argomento, v. S. Thobani, *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, p. 5 ss.; e, più di recente, C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021 p. 74 ss.; S. Thobani, *Il consenso al trattamento dei dati personali*, in Aa.Vv., *Manuale di diritto privato delle nuove tecnologie*, a cura di G. Magri, S. Martinelli e S. Thobani, Torino, 2022, p. 133 ss.

[16] Qui non è possibile richiamare per intero una letteratura divenuta, con il passare del tempo, praticamente sterminata. Senza nessuna pretesa di completezza, fra i sostenitori della natura autorizzativa del consenso, ci si limita pertanto a richiamare D. Messinetti, *Circolazione dei dati personali e disposizitivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv*., 1998, p. 339; A. Fici e E. Pellecchia, *Il consenso al trattamento*, in Aa.Vv., *Diritto alla riservatezza e circolazione dei dati personali,* I, a cura di R. Pardolesi, Milano, 2003, p. 469 ss.; S. Mazzamuto, *Il principio del consenso e il potere di revoca*, in Aa.Vv., *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, I, Milano, 2006, p. 993 ss., spec. pp. 1026-1027. Per un'articolata posizione attenta alla natura "negoziale" del consenso, v. G. Versaci, *Consenso al trattamento dei dati personali e dark patterns tra opzionalità e condizionalità*, in *Nuove leggi civ. comm*., 2022, p. 1130 ss.; Id., *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020, p. 61 ss., p. 137 ss., p. 168 ss.; e, con specifica attenzione al valore negoziale del rilascio di dati personali nell'ambito di una specifica operazione di consumo, vale a dire il contratto per la fornitura di contenuti o servizi digitali (v. direttiva 2019/770/UE), Id., *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. Sul punto, per una recente panoramica sulle diverse posizioni dottrinali, con un'apparente preferenza per l'approccio più negoziale, cfr. V. Bachelet, *Il consenso oltre il consenso*, Pisa, 2024, p. 76 ss.

ISBN 978-88-495-5568-4

si esauriscono con il (pur molto importante) dibattito sul consenso come condizione di liceità del trattamento (da coordinare peraltro, come si è detto, con le specifiche finalità perseguite, nel caso di specie, rappresentate dal *neuromarketing*)[17].

Già ai sensi dello stesso art. 9 (stavolta § 4) del GDPR, infatti, "gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute". In Italia, l'art. 2, c. 1, lett. f), del d.lgs. 10 agosto 2018, n. 101, ha disposto pertanto l'introduzione dell'art. 2-*septies* (rubricato "Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute") nel c.d. "codice della privacy". Alla luce dell'art. 2-*septies*, spetta al Garante per la protezione dei dati personali fissare ogni due anni, con un proprio provvedimento, le misure di garanzia (e le relative misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonimizzazione, le misure di minimizzazione, le specifiche modalità per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonché le eventuali altre misure necessarie a garantire i diritti degli interessati) per il trattamento dei dati genetici, biometrici e relativi alla salute. L'Autorità stessa vigila poi con attenzione sull'applicazione della normativa posta a protezione dei dati genetici, biometrici e relativi alla salute, sanzionando, se del caso, l'eventuale trattamento illecito[18]. E non è tutto.

In particolare, il titolare del trattamento – consultandosi con il responsabile della protezione dei dati (qualora, come sistematicamente avviene in casi del genere, ne sia stato designato uno *ex* art. 37 GDPR) – dev'effettuare, infatti, *una valutazione d'impatto* sulla protezione dei dati ai sensi dell'articolo 35 del GDPR (e delle «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679»)[19].

Inoltre, il titolare o il responsabile del trattamento – ed eventualmente il loro rappresentante – devono predisporre e tenere un registro delle attività di trattamento svolte sotto la responsabilità del titolare e, dietro richiesta, metterlo a disposizione dell'autorità di controllo (art. 30 del GDPR).

Infine, il titolare è chiaramente tenuto, specie nell'ottica del trattamento

[17] Sul punto, v., *infra*, § 3.2. ss.

[18] Un esempio recente è dato dal Provvedimento del 22 febbraio 2024, n. 9995680 (consultabile *online* sul sito ufficiale del Garante per la Protezione dei Dati Personali: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9995680*).

[19] Le «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679» (adottate il 4 aprile 2017, poi modificate e riadottate, da ultimo, il 4 ottobre 2017) contribuiscono ad integrare la disciplina sulla valutazione d'impatto contenuta nel GDPR (e sono facilmente consultabili online: *ec.europa.eu/newsroom/document.cfm?doc_id=47711*).

 ISBN 978-88-495-5568-4

di dati biometrici, anche alla consegna di un'informativa specifica funzionale all'eventuale rilascio proprio del consenso dell'interessato (art. 13 del GDPR).

La disciplina del GDPR sulla profilazione e sul trattamento dei dati biometrici delinea pertanto un panorama ancor oggi caratterizzato – oltre che da una serie di particolari tutele nonché misure di garanzia e di sicurezza – dalla centralità del ruolo del consenso dell'interessato, affiancato, però, dall'attenzione rivolta alle specifiche finalità. Non possiamo pertanto che proseguire nell'analisi guardando ai profili regolatori relativi ai casi dove il trattamento dei dati biometrici risulta specificamente funzionale al perseguimento di finalità di *marketing* (come avviene, per l'appunto, nell'ambito del *neuromarketing*)[20].

3.2. Se già la disciplina del GDPR sul trattamento dei dati biometrici non costituisce, come si è visto, un argomento privo di criticità, è però l'individuazione dell'esatto momento in cui l'attività di persuasione – accettabile – diviene una manipolazione – inaccettabile – della volontà dell'individuo a rappresentare senza dubbio l'aspetto maggiormente problematico del *neuromarketing*[21]. I rischi maggiori sono, infatti, «quelli della distorsione comportamentale e della discriminazione: le persone il cui comportamento viene, non semplicemente influenzato, bensì, distorto ossia manipolato, attraverso una comunicazione personalizzata che fa leva su loro specifiche e ben studiate caratteristiche e vulnerabilità decisionali e comportamentali, rischiano tipicamente di diventare persone diverse da quelle che sarebbero diventate se non fossero state fatte bersaglio di quella comunicazione»[22]. E ciò trova potenzialmente riscontri tanto nell'ambito della disciplina – ormai classica e, per alcuni profili, ancora "speciale" – del diritto dei consumi (§ 3.2.1.) quanto nell'odierno contesto normativo – in espansione e sempre più "generale" – del mondo digitale (§ 3.2.2.).

[20] Ci si muove così nel solco di chi, sviluppando la propria riflessione a partire dal ruolo del consenso nel trattamento dei dati, ha scelto però di sottolineare poi l'esigenza di soffermarsi anche sulla specifica finalità di *marketing*. Cfr., per tutti, S. Orlando, *Per un sindacato di liceità del consenso privacy*, cit., p. 536 ss.

[21] Lo sottolinea la stessa Commissione europea: "*From a policy perspective, understanding the exact point where acceptable persuasion becomes unacceptable manipulation is one of the crucial issues for the regulation of marketing and commercial practices, especially in the digital environment*" (European Commission, *State of the art of neuromarketing and its ethical implications*, cit., p. 27). Si tratta, in verità, di una sfida regolatoria "classica" posta anche dalle pratiche tradizionali di *marketing*: l'avvento delle nuove tecnologie dell'era digitale sembra limitarsi, da questo punto di vista, soltanto a rendere più complesso l'individuazione di un confine già di per sé difficile da tracciare.

[22] S. Orlando, *Per un sindacato di liceità del consenso privacy*, cit., p. 534.

ISBN 978-88-495-5568-4

3.2.1. Come noto, la differenza tra *influenza comportamentale* (ammessa, in linea di principio, laddove esercitata in conformità alla "diligenza professionale") e *distorsione comportamentale* (vietata, laddove conseguenza di pratiche contrarie alla "diligenza professionale") è stata normativamente tracciata, per la prima volta, con il divieto delle pratiche commerciali sleali, dalla direttiva 2005/29/CE[23]. Qui si sancisce, infatti, un divieto generale delle pratiche commerciali distorsive del comportamento economico dei consumatori (art. 5, dir. 2005/29/CE).

Questa previsione pone diverse problematiche con riferimento specifico al *neuromarketing*.

Ad emergere, fin da subito, è l'impossibilità di trovar un'univoca risposta alla domanda circa l'ammissibilità o meno di tutte le pratiche di *neuromarketing*. La valutazione dovrà essere fatta necessariamente nel merito, cercando d'intuire quando uno specifico strumento o, meglio ancora, un prodotto in una determinata circostanza finisce per spingersi oltre il confine della distorsione comportamentale. Anche per agevolare probabilmente tale valutazione è la stessa direttiva 2005/29/CE a prevedere, oltre al divieto di carattere generale, un elenco di quelle pratiche commerciali che sono considerate in ogni caso sleali (v. allegato I; peraltro, detto elenco si applica in tutti gli Stati membri e può essere modificato e integrato solo mediante revisione della direttiva). Nella maggior parte dei casi, spetterà però proprio all'interprete valutare se nel caso di specie si rientri o meno nell'ambito di applicazione del divieto sancito all'art. 5 della direttiva 2005/29/CE. Si tratta di una valutazione tutt'altro che semplice: non è detto, per esempio, che il soggetto che commercializza un determinato prodotto – che si avvale di tecniche di *neuromarketing* – sia effettivamente consapevole delle caratteristiche intrinseche del bene, rivelatesi poi più o meno distorsive del comportamento del consumatore (da cui l'ulteriore criticità relativa ad un'eventuale indagine supplementare sull'intera *supply chain*).

A ciò si aggiungono le perplessità riguardanti l'ambito di applicazione della direttiva. Anche se coordinata magari con importanti strumenti processuali di tutela collettiva, messi a disposizione tanto dal legislatore nazionale quanto da quello eurounitario[24], la direttiva 2005/29/CE può assicurar

[23] Per una riflessione che suggerisce di guardare la disciplina della protezione dei dati sempre con attenzione alla prospettiva consumeristica, v. Ch. Aubert-Hassouni, J. Clorarec, *Privacy Regulation in the Age of Artificial Intelligence*, in *The SAGE Handbook of Digital Marketing*, A. Hanlon, T.L. Tuten eds., SAGE, Los Angeles, London, New Delhi, Singapore, Washington DC, Melbourne, 2022, p. 544 ss.

[24] Il riferimento è rivolto alle recenti normative nazionali ed eurounitarie di tutela collettiva dirette ad introdurre la c.d. "*class action*" e la c.d. "azione rappresentativa". In Italia, il consumatore leso da una pratica scorretta ha a sua disposizione lo strumento dell'azione di classe, disciplinata dagli artt. 840-*bis* ss. c.p.c. In origine, l'azione di classe era disciplinata dall'art. 140-*bis* cod. cons. ed era esperibile soltanto dai consumatori (singoli, ovvero dalle

 ISBN 978-88-495-5568-4

un'efficace tutela soltanto dei consumatori, trovando applicazione nei rapporti cc.dd. *business-to-consumer* (o, più sinteticamente, *b2c*). E nei casi in

associazioni di consumatori), in casi individuati dal medesimo articolo, tra i quali figurava il risarcimento del danno derivante dalle pratiche commerciali scorrette. La l. 12 aprile 2019, n. 31 ne ha poi trasfuso la disciplina – con significative modifiche – nel codice di procedura civile agli artt. 840-*bis* ss., estendendo la legittimazione attiva anche a soggetti che non rientrino nella categoria dei consumatori. All'art. 840-*bis* c.p.c. si prevede, infatti, che: «i diritti individuali omogenei sono tutelabili anche attraverso l'azione di classe, secondo le disposizioni del presente titolo. A tal fine un'organizzazione o un'associazione senza scopo di lucro i cui obiettivi statutari comprendano la tutela dei predetti diritti o ciascun componente della classe può agire nei confronti dell'autore della condotta lesiva per l'accertamento della responsabilità e per la condanna al risarcimento del danno e alle restituzioni». Quest'azione consente di alleggerire la difficoltà di soddisfare l'onere della prova in capo ai soggetti che rimangano vittime di una pratica commerciale scorretta posta in essere da una stessa impresa. L'azione di classe permette poi al soggetto acquirente di un dispositivo relativamente poco costoso di trovare comunque tutela mediante l'adesione all'azione intentata da altri o da una associazione di categoria. Infine, il minor tasso di 'immobilismo' dell'acquirente potrebbe produrre un ulteriore effetto positivo sulle imprese responsabili giacché consapevoli di poter essere, sempre più spesso, chiamate a risarcire i danni. Sulla nuova azione di classe, si vedano, per tutti, C. Consolo, *L'azione di classe, trifasica, infine inserita nel c.p.c.,* in *Riv. dir. proc.*, 2020, p. 714 ss.; I. Pagni, *La class action riformata - L'azione inibitoria collettiva,* in *Giur. it*., 2019, p. 2297 ss. Per una panoramica più ampia, v. Aa.Vv., *Class action. Commento sistematico alla legge 12 aprile 2019, n. 31*, a cura di B. Sassani, Pisa, 2019, p. 1 ss.; S. Brazzini e P.P. Muià, *La nuova class action alla luce della legge 12 aprile 2019, n. 31*, Torino, 2019, spec. p. 63 ss. A proposito dei nuovi procedimenti collettivi nel codice di procedura civile, v. A. Carratta, *I nuovi procedimenti collettivi: considerazioni a prima lettura*, in *Giur. it*., 2019, p. 2297 ss.; D. Amadei, *Nuova azione di classe e procedimenti collettivi nel codice di procedura civile (l. 12 aprile 2019, n. 31),* in *Nuove leggi civ. comm*., 2019, 1049 ss.; A. Tedoldi e G.M. Sacchetto, *La nuova azione inibitoria collettiva ex art. 840-sexiesdecies c.p.c.*, in *Riv. dir. proc.*, 2021, p. 230 ss. e, per uno studio monografico, N. Rumine, *Natura e forme civilistiche di tutela degli interessi collettivi dei consumatori*, Pisa, 2022, p. 17 ss.

A partire dal 25 giugno 2023, la protezione del consumatore è garantita pure mediante la nuova c.d. "azione rappresentativa". Si tratta di un rimedio, delineato dalla direttiva 2020/1828/UE, con il fine di tutelare gli interessi collettivi dei consumatori in caso di violazione di alcune normative europee (tra le quali, ancora una volta, spicca la direttiva 2005/29/CE). Anche in questo caso non si intende approfondire la disciplina di tale strumento, ma soltanto evidenziarne le caratteristiche fondamentali (delineate dagli artt. 140-ter ss. del rinnovato codice del consumo). In *primis*, siffatta azione non è esperibile dal singolo consumatore, bensì soltanto dagli enti legittimati (v. art. 140-*quater* cod. cons.). Questi organismi, ai sensi dell'art. 140-*septies*, hanno la facoltà di agire anche in assenza di un mandato del singolo, allo scopo di ottenere provvedimenti inibitori (art. 140-*octies* cod. cons.), ovvero compensativi (art. 140-*novies* cod. cons.). Per quanto compatibile, la disciplina processuale cui tale strumento è sottoposto è quella di cui agli artt. 840-*bis* ss. c.p.c., contribuendo, a livello sistematico, a ridurre la diffusione di pratiche commerciali scorrette. Di recente, sulla portata della nuova Dir. 2020/1828/UE (e sui rapporti con la disciplina dell'azione di classe), cfr., *ex multis*, G. De Cristofaro, *Le 'azioni rappresentative' di cui agli artt. 140*-ter *ss. c.cons.: ambito di applicazione, legittimazione ad agire e rapporti con la disciplina generale delle azioni di classe di cui agli artt. 840-bis ss. c.p.c.,* in *Nuove leggi civ. comm*., 2024, p. 1 ss.; Id., *Azioni "rappresentative" e tutela degli interessi collettivi dei consumatori. La "lunga*

ISBN 978-88-495-5568-4

cui la commercializzazione di prodotti, che si avvale di strumenti e tecniche di *neuromarketing*, non coinvolge consumatori (si pensi, per esempio, ai fenomeni riconducibili all'applicazione di tali tecniche nell'ambito *business-to-business*, lavorativo o politico)? Sarà necessario, se del caso, guardar altrove.

Infine, non mancano, specie per il civilista, le criticità sul fronte rimediale. L'eventuale assoggettamento alla normativa eurounitaria in materia di pratiche commerciali sleali tra professionisti e consumatori – ossia al divieto generale previsto dall'art. 5 della direttiva 2005/29/CE e alle correlate sanzioni previste dalla direttiva (UE) 2019/2161 (c.d. "omnibus") per integrare sul punto la disciplina della predetta direttiva 2005/29/CE – non appare di certo come la panacea di tutti i mali. Con riferimento agli strumenti rimediali privatistici (che chiaramente non esauriscono le misure contenute nella normativa, come dimostra la presenza anche di rilevanti previsioni di carattere pubblicistico), assume un ruolo centrale il nuovo art. 11-*bis* direttiva 2005/29/CE: «[i] consumatori lesi da pratiche commerciali sleali devono avere accesso a *rimedi proporzionati ed effettivi, compresi il risarcimento del danno subito dal consumatore e, se pertinente, la riduzione del prezzo o la risoluzione del contratto. Gli Stati membri possono stabilire le condizioni per l'applicazione e gli effetti di tali rimedi*. Gli Stati membri possono tener conto, se del caso, della gravità e della natura della pratica commerciale sleale, del danno subito dal consumatore e di altre circostanze pertinenti»[25].

Purtroppo, l'ampia formulazione della norma con margini così significativi di discrezionalità (da esercitarsi in sede di recepimento da parte dei singoli legislatori nazionali) non sembra lasciare molte speranze circa

marcia" che ha condotto all'approvazione della dir. 2020/1828/UE e i profili problematici del suo recepimento nel diritto italiano, ivi, 2022, p. 1010 ss., spec. pp. 1033-1034; Id., *Legislazione italiana e contratti dei consumatori nel 2022: l'anno della svolta. Verso un diritto "pubblico" dei (contratti dei) consumatori?, ivi*, 2022, spec. pp. 44-45; E. Camilleri, *L'azione rappresentativa e il raccordo imperfetto con il diritto privato regolatorio. Le decisioni delle Authorities tra libero apprezzamento e presunzioni giurisprudenziali: spunti dall'arrêt Repsol, ivi*, 2024, p. 437 ss.; Id., *La dir. 2020/1828/UE sulle azioni rappresentative e il "sistema delle prove". La promozione dell'interesse pubblico attraverso la tutela degli interessi collettivi dei consumatori: verso quale modello di enforcement?*, *ivi*, 2022, p. 1052 ss., spec. p. 1058 ss.; M. Lorenzotti, *Azione di classe e diritti individuali omogenei: opportunità o limite?,* in *Contr. impr*., 2022, p. 682 ss.; F. Auletta, *L'azione rappresentativa come strumento di tutela dei diritti,* in *Nuove leggi civ. comm*., 2022, p. 1670 ss. Per alcune notazioni sintetiche sull'importante ruolo dell'azione di classe e dell'azione rappresentativa a tutela del consumatore nell'ipotesi di pratiche commerciali scorrette, cfr., di recente, M. D'Onofrio, *Il difetto di durabilità del bene*, Napoli, 2023, p. 133 ss.

[25] Infine, ai sensi dell'art. 11-*bis*, § 2, della direttiva 2005/29/CE, "detti rimedi non pregiudicano l'applicazione di altri rimedi a disposizione dei consumatori a norma del diritto dell'Unione o del diritto nazionale".

 ISBN 978-88-495-5568-4

l'applicazione di regole uniformi nel prossimo futuro. Nell'ordinamento italiano (che, seppure tardivamente, ha recepito la direttiva 2019/2161/UE, con il decreto legislativo 7 marzo 2023, n. 26), la via intrapresa – a fronte dell'ampio margine discrezionale lasciato dalla formulazione dell'art. 11-*bis* – risulta, per usare un eufemismo, "minimalista", limitandosi sostanzialmente a riportare, nell'ambito del nuovo art. 27, c. 15-*bis* del codice del consumo, le stesse parole dell'art. 11-*bis* della direttiva 2005/29/CE senza sciogliere nessuno dei nodi gordiani relativi ai presupposti e ai reciproci rapporti dei diversi rimedi prospettati dall'originaria formulazione eurounitaria ("I consumatori lesi da pratiche commerciali sleali possono altresì adire il giudice ordinario al fine di ottenere rimedi proporzionati ed effettivi, compresi il risarcimento del danno subito e, ove applicabile, la riduzione del prezzo o la risoluzione del contratto, tenuto conto, se del caso, della gravità e della natura della pratica commerciale sleale, del danno subito e di altre circostanze pertinenti. Sono fatti salvi ulteriori rimedi a disposizione dei consumatori").

Dall'analisi dell'odierna normativa (eurounitaria e nazionale) sulle pratiche commerciali sleali[26] emergono pertanto una serie d'indicazioni utili per delineare la disciplina del *neuromarketing*, ma, al contempo, diverse criticità riguardanti principalmente l'individuazione dell'inaccettabile distorsione del comportamento dell'individuo, l'ambito applicativo limitato ai rapporti con i consumatori e le caratteristiche specifiche (che difficilmente saranno uniformi a livello eurounitario) dei rimedi privatistici.

[26] Sulle pratiche commerciali "sleali" (definite poi, all'esito del recepimento nell'ambito dell'ordinamento italiano, "scorrette" nel codice del consumo), cfr., per tutti, G. De Cristofaro, voce *Pratiche commerciali scorrette*, in *Enc. dir., Annali*, V, Giuffrè, 2012, p. 1079 ss., spec. p.1086. Secondo l'Autore, "*non è chiaro per quale ragione il legislatore abbia preferito l'aggettivo «scorrette» all'aggettivo «sleali», che compariva invece nella versione italiana del testo della direttiva*. È possibile che tale opzione sia stata ispirata dall'intento di evidenziare anche a livello lessicale la diversità di ratio, obiettivi di tutela e ambito di applicazione delle nuove disposizioni attuative della direttiva, rispetto alla disciplina generale della concorrenza sleale contenuta negli art. 2598 ss. c.c. Non si può dire tuttavia che la scelta sia caduta sul termine più idoneo ad assicurarne la piena realizzazione. Non soltanto perché, a norma dell'art. 2598 n. 3 c.c., compie atti di concorrenza «sleale» chiunque si avvalga di mezzi non conformi ai principi della «correttezza» professionale e idonei a danneggiare l'altrui azienda, ma anche e soprattutto perché, all'interno del codice del consumo, i termini «lealtà» e «correttezza» vengono utilizzati entrambi – ora isolatamente (art. 52 comma 2 c. cons.: lealtà; art. 18 lett. d e art. 67-quater comma 2 c. cons.: correttezza), ora congiuntamente (art. 1 lett. c-bis e art. 39 c. cons.) – sempre in combinazione con la nozione di «buona fede» (oggettiva), senza che appaia possibile e ragionevole attribuire all'uno un significato e una portata non pienamente corrispondenti a quelli propri dell'atto. Anche in considerazione di ciò, *deve escludersi che la scelta di ricorrere all'aggettivo «scorrette» anziché all'aggettivo «sleali» possa avere ripercussioni di sorta*, sia ai fini della ricostruzione e dell'inquadramento sistematico del nuovo *corpus* normativo, sia ai fini dell'interpretazione delle singole disposizioni che lo compongono" (corsivo aggiunto).

ISBN 978-88-495-5568-4

3.2.2. Alla normativa delle pratiche commerciali scorrette sembra essersi poi recentemente affiancata una nuova disciplina. Si tratta dell'Artificial Intelligence Act (c.d. AI Act) – definitivamente approvato il 13 marzo 2024 e destinato a divenire applicabile, dopo la pubblicazione sulla Gazzetta ufficiale dell'Unione europea (prevista per la primavera 2024), per la maggior parte delle sue disposizioni, a due anni dalla sua entrata in vigore, fatta eccezione per le applicazioni vietate, rispetto alle quali risulterà applicabile già sei mesi dopo – che è diretto «to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of artificial intelligence systems (AI systems) in the Union, and to support innovation» (art. 1).

La nuova normativa – frutto di un susseguirsi di confronti serrati (e di differenti versioni testuali) – suggerisce una serie d'interessanti (e ulteriori) spunti di riflessione sulla disciplina del *neuromarketing*[27].

Nell'ottica (non sempre chiara) di disciplinare l'immissione sul mercato, la messa in servizio o l'uso di "sistemi di intelligenza artificiale"[28], l'*AI Act* delinea un'articolata disciplina della materia incentrata su un approccio orizzontale c.d. "*risk-based*": più alto è il coefficiente di rischio legato all'utilizzo di un determinato sistema, più severa ne risulterà la regolamentazione[29].

Non c'è dubbio che la disciplina del trattamento dei dati biometrici (specie su larga scala) abbia rappresentato – come testimoniato dai numerosi Considerando dedicati all'argomento (v., fra i tanti, i nn. 12, 14, 15, 16, 17, 18, 29, 30) nonché dalle diverse versioni testuali emerse nel c.d. "trilo-

[27] Nell'ottica di regolare il fenomeno suggerisce di valorizzare, oltre alla disciplina del GDPR, le più recenti normative eurounitarie del *Digital Services Act* e dell'*AI Act* anche L. Sposini, *Neuromarketing and Eye-Tracking Technologies Under the European Framework: Towards the GDPR and Beyond,* in *Journal of Consumer Policy*, 2024 (pubblicato in open access il 26 gennaio 2024 e reperibile online: *https://link.springer.com/article/10.1007/s10603-023-09559-2#article-info*). Per un'impostazione attenta ai diversi testi normativi eurounitari, letti anche alla luce di una prospettiva interdisciplinare, v. S. Fassiaux, *Preserving Consumer Autonomy through European Union Regulation of Artificial Intelligence: A Long-Term Approach*, in *European Journal of Risk Regulation*, 2023, p. 1 ss.

[28] Secondo l'ultima definizione, cristallizzata nell'odierno art. 3, n. 1 dell'AI Act, "'*AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*".

[29] Per alcuni spunti critici, anche a partire dall'adozione dell'approccio c.d. "*risk based*", v., *ex multis*, E.M. Incutti, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale*, cit., p. 535 ss.

 ISBN 978-88-495-5568-4

go" tra Parlamento Europeo, Commissione e Consiglio[30] – uno dei profili più discussi nell'ambito dell'elaborazione e poi della formulazione definitiva dell'*AI Act*. Tuttavia – fermo restando la particolare delicatezza (già evidenziata dall'analisi del GDPR) dell'oggetto del trattamento (rappresentato dai dati biometrici) – risulta adesso fondamentale, ai fini della presente riflessione, prender in considerazione l'approccio regolatorio eurounitario nei confronti dei "sistemi di riconoscimento delle emozioni" (cioè, ai sensi dell'art. 3, n. 39 dell'Act, sistemi di IA finalizzati all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici) così da perseguire specificamente finalità di *marketing*.

Il c.d. "neuromarketing", infatti, pone certamente al giurista sfide "nuove" assieme, però, a sfide ormai divenute "classiche". Il *neuromarketing* consente, infatti, di muoversi all'esito di un'analisi più precisa: il *marketer* rischia sicuramente di più trattando dati biometrici, ma può contare, per altro verso, su strumenti tecnologici sempre più avanzati e soprattutto su un'evidenza scientifica che gli consente d'influenzare più incisivamente la volontà del singolo individuo. Ai nuovi rischi e strumenti del *neuromarketing* si affiancano così le questioni classiche legate alla finalità stessa del trattamento circa l'opportuno discrimine da individuare fra l'attività di persuasione accettabile e quella di distorsione inaccettabile per l'ordinamento. È pertanto nella duplice prospettiva delle sfide nuove e classiche poste dal *neuromarketing* che meritano di essere prese in considerazione le recenti previsioni dell'AI Act.

A cominciare – com'è già stato sottolineato anche con riferimento alle precedenti versioni dell'AI Act[31] – dall'art. 5 (rubricato "*Prohibited AI Practices*"). Qui non è dato riscontrare nessun riferimento specifico alla finalità di *marketing* (né tanto meno di *neuromarketing*), ma diversi spunti di riflessione emergono lo stesso dall'odierna formulazione perlomeno delle lett. a), b) e f) delle pratiche vietate ai sensi dell'art. 5 dell'AI Act.

Innanzitutto, ai sensi della lett. a), è vietata "*the placing on the market, the putting into service or the use of an AI system* that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially *distorting the behaviour* of a person or a group of persons by appreciably

[30] Le diverse versioni del testo dell'*AI Act* (assieme a molti altri documenti di grande interesse ai fini dell'analisi e dell'interpretazione dell'intervento normativo eurounitario) sono facilmente reperibili *online* al sito: *https://artificialintelligenceact.eu/*.

[31] Per un'analisi complessiva della disciplina del neuromarketing nell'ambito delle precedenti proposte dell'*AI Act*, v. S. Orlando, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di* Artificial Intelligence Act, cit., p. 346 ss.; E.M. Incutti, *Sistemi di riconoscimento delle emozioni e ruolo dell'autonomia privata: linee evolutive di un umanesimo digitale*, cit., p. 527 ss.; L. Sposini, *Neuromarketing and Eye-Tracking Technologies Under the European Framework: Towards the GDPR and Beyond*, cit.

ISBN 978-88-495-5568-4

impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons *significant harm*". Ne deriva un divieto che, pur non richiamando espressamente la finalità di *marketing*, sembra farvi (almeno implicitamente) riferimento. Qui – lungi dallo sviluppare un'analisi approfondita della previsione, che sicuramente imporrà un confronto serio fra teorici e pratici negli anni a venire – non è possibile trascurare del tutto la struttura stessa del divieto. Si delineano, infatti, delle condotte vietate (l'immissione sul mercato, la messa in servizio o l'uso di un sistema di intelligenza artificiale che utilizzi tecniche subliminali al di là della coscienza di una persona o tecniche manipolative o ingannevoli)[32], caratterizzate dall'obiettivo, o anche solo dall'effetto, di *distorcere* (come si è già visto, in altro contesto, con riferimento alle pratiche commerciali sleali) il comportamento di una persona o di un gruppo di persone. Tale manipolazione della volontà – per essere vietata – dev'essere poi in grado di causare un *danno significativo* a quella persona, a un'altra persona o a un gruppo di persone.

Alla (complessa) categoria delle persone o dei gruppi di persone *vulnerabili* è poi specificamente dedicata la previsione di cui alla lett. b)[33], che, richiamando per il resto sostanzialmente la struttura della lett. a), vieta «*the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities* of a person or a specific group of

[32] Non è chiaro, per esempio, il significato che si vuole attribuire all'avverbio "*purposefully*" (volutamente). Quest'ultimo risulta giustapposto, almeno in apparenza, alle tecniche manipolative o ingannevoli, ma logicamente dovrebbe forse esser accostato alla condotta dell'agente.

[33] Alla vulnerabilità è giustamente dedicata un'ampia attenzione nell'ambito dell'AI Act (che, però, non ne fornisce una definizione chiara). Tale profilo assume un rilievo particolarmente significativo nell'analisi delle possibili conseguenze pregiudizievoli del neuromarketing. Lo rilevano – oltre alla stessa Commissione europea (*State of the art of neuromarketing and its ethical implications*, cit., spec. pp. 18 ss., 26) – A. Al Abbas, W. Chen e M. Saberi, *The Impact of Neuromarketing Advertising on Children: Intended and Unintended Effects*, in *KnE Social Sciences*, 2019, pp 1 ss. Per alcuni interessanti spunti sui soggetti vulnerabili, v. B. Gardella Tedeschi, *L'indagine giuridica*, in V. Cappellato, B. Gardella Tedeschi e E. Mercuri, *Anziani. Diritti, bisogni, prospettive. Un'indagine sociologica e giuridica*, Il Mulino, Bologna, 2021, p. 181 ss., spec. p. 192, p. 206 ss.; M.G., Bernardini, *Il soggetto vulnerabile. Status e prospettive di una categoria (giuridicamente) controversa*, in *Riv. fil. dir*., 2017, p. 365 ss.; N. Zorzi Galgano, *Il consumatore medio ed il consumatore vulnerabile nel diritto comunitario*, in *Contr. impr./Eur*., 2010, p. 549 ss., 587 ss.; R. Incardona e C. Poncibò, *The Average Consumer, the Unfair Commercial Practices Directive, and the Cognitive Revolution*, in *Journal of Consumer Policy Issue*, 30, 2007, p. 21 ss.; e, nella letteratura straniera, v. M. Fineman, «*Elderly» as vulnerable: Rethinking the nature of individual and societal responsibility*, in *Elder Law Journal*, 2012, 20, p. 71 ss.; T. Mattsson e M. Katzin, *Vulnerability and ageing*, in A. Numhauser-Henning (ed.), *Elder Law. Evolving European Perspectives*, London, 2017, p. 113 ss.

 ISBN 978-88-495-5568-4

persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of *materially distorting the behaviour* of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person *significant harm».*

Nell'ottica della presente riflessione può risultar interessante, infine, richiamare la lett. f) dell'art. 5 dell'AI Act, laddove si vieta «*the placing on the market, the putting into service for this specific purpose, or the use of AI systems to infer emotions of a natural person in the areas of workplace and education institutions*, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons». Si tratta – fermo restando l'attuale formulazione (stilisticamente migliorabile) – di un divieto rivolto al riconoscimento (e al possibile conseguente sfruttamento) delle emozioni delle persone nell'ambiente lavorativo e formativo, fatta eccezione per il ricorso a sistemi d'intelligenza artificiale sviluppati per essere collocati sul mercato per scopi relativi alla tutela della salute o della sicurezza[34].

Nell'ultima versione dell'art. 5 dell'AI Act se, per un verso, manca ancora un riferimento specifico alla finalità-tabù di *marketing*[35], per un altro, sono vietate ormai (anche espressamente) condotte basate sul riconoscimento delle emozioni ben al di fuori del "classico" rapporto consumeristico[36].

Altre notazioni interessanti sulla disciplina del *neuromarketing* sembrano poter provenire poi dall'analisi della regolamentazione – contenuta sempre nell'AI Act (v. *Chapter* III) – dei sistemi d'intelligenza artificiale ad alto rischio. Questi, prima di essere introdotti o utilizzati nell'UE, sono sottoposti dall'AI Act a rigorosi controlli con la previsione di una serie di requisiti e obblighi (cui sono assoggettati non soltanto i fornitori dei sistemi di IA, ma anche gli altri attori lungo la catena del valore dell'IA, come, per esempio, importatori, distributori e rappresentanti autorizzati). Alla luce del potenziale alto rischio associato a tali applicazioni, gli obblighi

[34] Sembra così trovar accoglimento nel testo normativo il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo per la protezione dei dati (EDPB-GEPD) n. 5/2021 del 18 giugno 2021 sulla proposta di *Artificial Intelligence Act*, secondo cui "l'utilizzo dell'IA per dedurre le emozioni di una persona fisica sia assolutamente inopportuno e dovrebbe essere vietato, ad eccezione di taluni casi d'uso ben specificati, ossia per finalità sanitarie o di ricerca (ad esempio pazienti per i quali il riconoscimento delle emozioni è rilevante), sempre applicando idonee tutele e, naturalmente, nel rispetto di tutte le altre condizioni e restrizioni relative alla protezione dei dati, compresa la limitazione delle finalità" (il documento è consultabile per intero al seguente indirizzo: *https://www.edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf*; v. spec. p. 14, punto 35).

[35] Il "tabù del *marketing*" nella disciplina dell'AI Act è stato sottolineato in modo critico da S. Orlando, *Regole di immissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act*, cit., p. 356 ss.

[36] V., *supra*, § 3.2.1.

ISBN 978-88-495-5568-4

imposti sono significativi ed includono l'adozione di sistemi di gestione dei rischi, il rispetto di requisiti relativi alla (necessariamente elevata) qualità dei *dataset* utilizzati nonché all'adozione della documentazione tecnica e alla conservazione delle registrazioni, alla trasparenza e alla fornitura di informazioni agli utenti. L'AI Act prescrive poi l'adozione di adeguati livelli di accuratezza, robustezza e cybersicurezza, richiedendo che gli operatori effettuino anche una valutazione dell'impatto sui diritti fondamentali prima che i sistemi di IA ad alto rischio siano immessi sul mercato.

Nell'ambito dei sistemi d'IA ad alto rischio viene fatta rientrare una vasta gamma di dispositivi (v. spec. Allegato III). Innanzitutto, un ruolo centrale è riconosciuto – come sistemi d'IA ad alto rischio – agli strumenti di identificazione biometrica, categorizzazione e riconoscimento delle emozioni (Allegato III, punto 1)[37]. Non solo. Un interessante riferimento, seppur implicito, riguarda pure il c.d. "marketing politico", che sembra fare capolino, laddove si considerano ad alto rischio (Allegato III, punto 8, lett. b) «AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda […]».

Emergono così – pur in assenza di una disciplina organica – diversi indici normativi che, seppur in ordine sparso, cominciano a delineare una regolamentazione del *neuromarketing*. Il ricorso a tali strumenti e tecniche – sebbene all'esito di una formulazione legislativa talvolta, ancor oggi, poco chiara – sembra complessivamente ammesso, ma circondato da rilevanti cautele. L'attuale AI Act delinea così una disciplina che, pur non regolando sistematicamente il *neuromarketing*, risulta consapevole delle complesse problematiche sottese[38], consentendo, ad una prima lettura, il ricorso circostanziato a tali strumenti purché non produttivi di un'inaccettabile distorsione della volontà di una persona (o di un gruppo di persone), specie se vulnerabile, in un modo che le causa o è probabile che le causi un danno significativo. Tali previsioni risultano, infine, presidiate da rilevanti sanzioni pubblicistiche (v. artt. 99 ss. AI Act), cui sembrano doversi affiancare, seppur implicitamente, rimedi contrattuali e risarcitori (rimessi, però,

[37] Ciò non toglie che, secondo diversi osservatori, tale disciplina risulti lo stesso troppo lassista nei confronti delle multinazionali del settore tecnologico. Per alcune primissime voci critiche (non più sulla Proposta di *AI Act*, ma direttamente) con riferimento al testo definitivo dell'*AI Act* (e a come si sarebbe potuto fare di più nell'ottica di una tutela dei dati biometrici delle persone), cfr. *https://www.accessnow.org/press-release/ai-act-failure-for-human-rights-victory-for-industry-and-law-enforcement/*; *https://reclaimyourface.eu/eu-ai-act-will-fail-commitment-to-ban-biometric-mass-surveillance/*.

[38] L'esistenza (ed il tono complessivo) dello stesso documento della Commissione UE (*State of the art of neuromarketing and its ethical implications*, cit.), già più volte richiamato, conferma la preoccupata consapevolezza delle stesse istituzioni europee nei confronti dei diversi profili problematici del *neuromarketing*.

 ISBN 978-88-495-5568-4

ai futuri interventi normativi di livello eurounitario e alle diverse disposizioni legislative nazionali) ancor oggi poco chiari[39].

4. Anche tralasciando le possibili criticità relative al contemperamento della nuova normativa con la disciplina specifica (approvata pressoché contestualmente) sulla pubblicità politica – laddove sembra di riscontrare un assoluto divieto di ricorso a tecniche di *targeting* (e, di conseguenza, d'influenza) che implicano il trattamento di categorie particolari di dati[40] – l'articolazione

[39] Non è possibile, al riguardo, evitare ogni riferimento alla Proposta di direttiva del 28 settembre 2022 – ancor oggi in via di definizione e chiamata ad adattare, fra l'altro, le regole della responsabilità civile all'intelligenza artificiale – nonché le numerose (e spesso diverse fra loro) normative nazionali su regole e rimedi risarcitori.

[40] Nell'ambito della nuova normativa ("*Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising*") sono fissate delle condizioni rigorose per consentire la pubblicità politica mirata online. I dati devono essere raccolti dall'interessato e possono essere utilizzati solo dopo che quest'ultimo ha dato un consenso esplicito e separato per il loro utilizzo ai fini di pubblicità politica. Le categorie particolari di dati personali – ai sensi degli artt. 9 e 10 del GDPR (si pensi, per esempio, oltre ai dati biometrici, a quelli che rivelano l'origine razziale o etnica o le opinioni politiche) – non possono essere utilizzate per la profilazione. Non è qui possibile riportare per intero la normativa (contenuta nel Chapter III, "Targeting and ad delivery of online political advertising"). Ci si limita pertanto, ai nostri fini, soltanto all'art. 18 (Specific requirements related to targeting techniques and ad-delivery techniques in the context of online political advertising – (1). Targeting techniques or ad-delivery techniques that involve the processing of personal data in the context of online political advertising shall be permitted only when the following conditions are fulfilled: (a) the controller collected the personal data from the data subject; (b) the data subject has provided explicit consent within the meaning of Regulations (EU) 2016/679 and (EU) 2018/1725 to the processing of personal data separately for the purpose of political advertising; and (c) those techniques do not involve 'profiling' as defined in Article 4, point 4, of Regulation (EU) 2016/679 and in Article 3, point 5, of Regulation (EU) 2018/1725 using special categories of personal data referred to in Article 9(1) of Regulation (EU) 2016/679 and in Article 10(1) of Regulation (EU) 2018/1725. (2). In the context of political advertising, targeting techniques or ad-delivery techniques that involve the processing of the personal data of a data subject that is known by the controller with reasonable certainty to be at least one year under the voting age established by national rules are prohibited. Compliance with the obligations set out in this paragraph shall not oblige the controller to process additional personal data in order to assess whether the data subject is one year under the voting age. (3). This Article shall not apply to communications of any political party, foundation, association or any other non-profit body, to their members and former members or to communications, such as newsletters, linked to their political activities, as long as those communications are solely based on subscription data and therefore strictly limited to their members, former members or subscribers and are based on personal data provided by them and do not involve processing of personal data to target or otherwise further select the recipients and the messages they receive. (4). For the purposes of implementing the requirements of Regulations (EU) 2016/679 and (EU) 2018/1725 on providing explicit consent, as well as on withdrawing it once given, controllers shall make sure that: (a) the data subject is not requested to consent if he or she has already indicated by automated means that he or she does not consent to data processing for political advertising purposes,

ISBN 978-88-495-5568-4

complessiva dell'AI Act sembra però sollevare delle problematiche non irrilevanti di coordinamento soprattutto con riferimento al divieto generale tratteggiato nel c.d. "*Digital Sevices Act*" (*Regulation* (EU) 2022/2065 *of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC*).

Quest'ulteriore testo normativo eurounitario è rivolto notoriamente a contribuire al corretto funzionamento del mercato interno dei servizi intermediari, stabilendo norme armonizzate per un ambiente *online* sicuro, prevedibile e affidabile che faciliti l'innovazione e assicuri la tutela effettiva dei diritti fondamentali sanciti dalla Carta (compreso il principio della protezione dei consumatori).

Il *Digital Services Act* – consapevole che le piattaforme *online*, in quanto ambienti particolarmente sensibili per inserzioni pubblicitarie basate su tecniche di *targeting* ottimizzate con riferimento ai destinatari del servizio per soddisfare i loro interessi e potenzialmente attirare le loro vulnerabilità, presentano un rischio più elevato (per i singoli come per la società nel suo complesso) con effetti negativi potenzialmente molto gravi (si pensi, per esempio, ai margini per eventuali campagne di disinformazione o discriminazione di determinati gruppi)[41] – si muove nella direzione di precludere ai fornitori delle piattaforme di presentare inserzioni pubblicitarie basate sulla profilazione realizzata trattando categorie particolari di dati personali

unless the request is justified by a substantial change of circumstances; (b) the data subject who does not give his or her consent is to be offered an equivalent alternative for using the online service without receiving political advertising.") e al Considerando 25 ("Commercial advertising and marketing practices can legitimately affect consumers' perceptions of products and services or their buying behaviour, including through brand differentiation based on company actions in the field of corporate social responsibility, delivering social impact, or any other types of purpose-driven engagement. This Regulation should apply to commercial advertising that is liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process").

[41] Tale consapevolezza del legislatore eurounitario emerge, in particolare, alla lettura del Considerando 69 del *Digital Services Act* ("Quando ai destinatari del servizio vengono presentate inserzioni pubblicitarie basate su tecniche di targeting ottimizzate per soddisfare i loro interessi e potenzialmente attirare le loro vulnerabilità, ciò può avere effetti negativi particolarmente gravi. In alcuni casi, le tecniche di manipolazione possono avere un impatto negativo su interi gruppi e amplificare i danni per la società, ad esempio contribuendo a campagne di disinformazione o discriminando determinati gruppi. Le piattaforme online sono ambienti particolarmente sensibili per tali pratiche e presentano un rischio per la società più elevato. Di conseguenza, i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione, come definite all'articolo 4, punto 4), del regolamento (UE)2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, dello stesso regolamento, anche utilizzando categorie di profilazione basate su tali categorie speciali. Tale divieto lascia impregiudicati gli obblighi applicabili ai fornitori di piattaforme online o a qualsiasi altro fornitore di servizi o inserzionista coinvolti nella diffusione della pubblicità a norma del diritto dell'Unione in materia di protezione dei dati personali").

 ISBN 978-88-495-5568-4

(compresi chiaramente quelli biometrici). Ne deriva il perentorio divieto – scolpito (più che sancito) a chiare lettere all'art. 26, § 3 (dedicato alla "pubblicità sulle piattaforme online") – secondo cui "i fornitori di piattaforme online non possono presentare pubblicità ai destinatari del servizio basate sulla profilazione, quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679, utilizzando le categorie speciali di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE)2016/679".

L'imposizione di un divieto del genere – a prescindere dall'effettiva capacità interdittiva delle condotte pregiudizievoli[42] – risulta sicuramente espressione di un'opzione legislativa di segno diverso dall'assetto più articolato (e frastagliato) complessivamente delineato dall'AI Act. Quest'apparente contraddizione sottolinea, in ogni caso, l'esigenza di un opportuno maggiore coordinamento – forse possibile a seguito di un ulteriore sforzo interpretativo[43] – fra le due normative così da poter pensare finalmente a delineare poi un vero e proprio sistema eurounitario della materia.

5. Secondo uno studio recente della Commissione europea, "*the main problem is that the neuromarketing sector is very unregulated*"[44]. Oggi, in realtà, sembra di esser in presenza, più che di un *deficit* assoluto di regolamentazione, di una sorta di "*patchwork*" di disposizioni di matrice eurounitaria che impone all'interprete un momento di riflessione.

Ormai consapevole delle numerose problematiche sottese al fenomeno, il legislatore eurounitario, infatti, sembra essersi mosso – soprattutto di recente – per assicurare una disciplina (almeno parziale) dei diversi profili del *neuromarketing*. Così alla normativa di protezione dei dati personali e, in particolare, dei dati biometrici non si è affiancata soltanto la disciplina delle pratiche commerciali sleali – applicabile, nonostante una serie di difficoltà interpretative, nei rapporti *b2c* – ma anche le numerose recenti previsioni – non sempre perfettamente coordinate fra loro – contenute soprattutto nell'*Artificial Intelligence Act* e nel *Digital Services Act*.

[42] Tale divieto rischia di risultare, al contempo, fin troppo *tranchant* (poiché apparentemente sempre applicabile ai fornitori di piattaforme online anche in assenza di un elemento soggettivo della loro condotta) e suscettibile di un'elusione relativamente semplice (avvalendosi magari dell'assenza di disciplina o della presenza di regole meno rigorose che caratterizzano ambiti diversi, ma comunque limitrofi, rispetto a quello disciplinato dal *Digital Services Act*).

[43] Si potrebbe forse avanzare una possibile lettura dell'art. 26, § 3, del DSA come "speciale" rispetto alla disciplina dell'*AI Act* alla luce della suddetta particolare pericolosità di tali condotte in un ambiente (quello delle piattaforme online) considerato particolarmente sensibile nei confronti di tali pratiche, potendo comportare una maggiore rischiosità per l'intera società (si pensi, per esempio, ad eventuali campagne di disinformazione e/o di discriminazione di determinati gruppi; v., supra, nt. 41 e Considerando 69 del DSA).

[44] European Commission, *State of the art of neuromarketing and its ethical implications*, cit., p. 26.

ISBN 978-88-495-5568-4

Dall'analisi condotta emerge una disciplina ancora frammentata ed in evoluzione costante come dimostrato dalla molteplicità dei testi normativi coinvolti nonché dal contenuto delle diverse disposizioni (e delle differenti versioni che hanno caratterizzato tali testi durante i vari passaggi dell'*iter* legislativo eurounitario). L'impressione è pertanto che la posizione dell'Unione europea sul *neuromarketing* (ma probabilmente, più in generale, sui fenomeni che si avvalgono di nuove tecnologie digitali) sia ancor oggi in una fase di consolidamento[45].

Il legislatore eurounitario si è preoccupato, infatti, di trovar un equilibrio fra le istanze di tutela delle persone e del mercato, confidando in un rinnovato "Brussels effect" (cioè nell'ormai noto processo di globalizzazione normativa unilaterale causato dall'Unione Europea che finisce per esternalizzare le sue regole al di fuori dei propri confini attraverso meccanismi di mercato)[46], ma consapevole, al contempo, delle sfide regolatorie poste da altre normative (a partire, per esempio, da quella statunitense sull'intelligenza artificiale e sui dati biometrici, incentrata su un approccio più *business friendly*, al fine d'incentivare al massimo, senza rigide regolamentazioni, lo sviluppo dell'imprenditoria digitale e il mantenimento del suo primato tecnologico mondiale)[47].

Nonostante le persistenti difficoltà ricostruttive di una disciplina ancor oggi poco sistematica, sembra possibile, all'esito dell'analisi finora condotta, rintracciare conclusivamente delle possibili linee evolutive dell'odierno sistema normativo.

Innanzitutto, l'*intentio legis* sembra orientata a disciplinare il fenomeno

[45] Non è questa la sede per evidenziare tutti gli spunti normativi che sembrano indirizzare l'interprete in tal senso. Ci si limita a rilevare, oltre alle notazioni sviluppate nel testo, l'evidente opzione di politica legislativa eurounitaria favorevole allo sviluppo dello strumento della c.d. "*sandbox*" (mutuando così in ambito regolatorio la "sabbiera", cioè il recinto della sabbia destinato ai giochi dei bambini). Attraverso l'introduzione e lo sviluppo di tale strumento normativo si vuole configurare un ambiente delimitato dov'è possibile osservare, così da potere meglio comprendere e poi regolare, le conseguenze derivanti dall'evoluzione e dalla sperimentazione tecnologica in un determinato mercato. Quest'opzione, che merita ben altro genere di riflessione sistematica, è stata già adottata con riferimento alla disciplina delle nuove tecnologie in diversi ambiti: si pensi, per esempio, al settore finanziario (c.d. "*FinTech*"; v. decreto del Ministero dell'Economia e delle Finanze, 30 aprile 2021, n. 100, attuativo della delega prevista dal decreto-legge 30 aprile 2019, n. 34, convertito, con modificazioni, dalla legge 28 giugno 2019, n. 58, nonché il Provvedimento della Banca d'Italia 3 novembre 2021) o, per l'appunto, alle cc.dd. "*AI Sandboxes*" (di cui agli artt. 53 ss. dell'*AI Act*).

[46] Sul punto, cfr., per tutti, G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2024, p. 113 ss.

[47] La richiamata disciplina statunitense, anch'essa frammentata, è contenuta in una pluralità di testi normativi, fra cui, per esempio, il "*Blueprint for an AI Bill of rights*" dell'ottobre del 2022 e l'"*Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*", n. 14110, firmato dal Presidente Biden il 30 ottobre 2023.

 ISBN 978-88-495-5568-4

del *neuromarketing*, per un verso, prendendo in considerazione le sfide nuove legate a sistemi di IA finalizzati all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici e, per un altro, fronteggiando le sfide classiche riconducibili all'individuazione complessa dei casi di manipolazione inaccettabile della volontà delle persone, o di gruppi di persone, specie se vulnerabili.

Inoltre, l'assetto normativo eurounitario presidia sempre le regole dei diversi profili del *neuromarketing* con una serie di diverse sanzioni e tutele. Queste sono state predisposte, dapprima, prevalentemente nel contesto dei contratti *b2c*, poi, in una serie sempre più ampia di rapporti fra privati.

Infine, accanto alle rilevanti sanzioni di carattere pubblicistico, non deve trascurarsi il ruolo (sebbene non ancora chiaramente definito) dei rimedi di stampo privatistico: si pensi, oltre ai possibili strumenti contrattuali a protezione della libertà contrattuale nonché dell'autodeterminazione del contraente (e ascrivibili, secondo parte della dottrina, soprattutto alla categoria della nullità)[48], alle azioni risarcitorie chiamate a fronteggiare le condotte vietate.

Nell'ottica di riordinare le risposte fornite in ordine sparso dall'ordinamento eurounitario – apparentemente orientato nel senso di consentire la diffusione di strumenti di *neuromarketing* circondandoli, come si è visto, di misure e cautele varie presidiate da sanzioni pubblicistiche e rimedi privatistici – sembra così destinato ad emergere nuovamente il ruolo del giurista, chiamato ad aiutare gli operatori del settore nel governare l'evoluzione del fenomeno anche nei rapporti fra privati. Al riguardo – secondo l'insegnamento, ancor oggi attuale, di Michele Giorgianni – "spetta alla dottrina privatistica il gravoso ma insieme stimolante compito di adeguare i propri strumenti teorici al nuovo volto del diritto privato"[49].

[48] Sul punto, v. L. Tafaro, *Neuromarketing e tutela del consenso*, Napoli, 2018, pp. 128 ss., 181 ss., spec. pp. 186-187.

[49] M. Giorgianni, Il *diritto privato ed i suoi attuali confini ("prolusione" accademica letta a Napoli nel 1961*), cit., 2012, p. 2943 ss., spec. p. 2946.

ISBN 978-88-495-5568-4

Mario Renna

L'identità sicura: il banco di prova del *data breach*

Sommario: 1. Sicurezza e violazione dei dati personali: la valenza del principio. – 2. *Data breach*: trasparenza e reazione. – 3. Le *Guidelines 9/2022 on personal data breach notification under GDPR*. – 4. Considerazioni conclusive.

1. Il Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, sin d'ora GDPR, posiziona la sicurezza tra i principi applicabili al trattamento dei dati personali, quindi al vertice della regolamentazione giuridica[1]: i dati personali necessitano di essere trattati in maniera tale da assicurare una adeguata sicurezza e una costante integrità e riservatezza [art. 5, § 1, lett. *f*)].

Il principio di sicurezza si atteggia a dispositivo giuridico che necessita di una concretizzazione puntuale e, al contempo, favorisce l'emergere di una serie di responsabilità gravanti sul titolare e sul responsabile del trattamento[2]. Per costoro si impone una valutazione costante e prudente dei rischi[3]: con riferimento ad ogni fase dell'attività del trattamento dei dati, si

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

[2] Corte giust., 14 dicembre 2023, C-340/21, con nota di M. Renna, *I dati personali al sicuro: diritti, responsabilità, tutele*, in *Foro it.*, 2024, IV, c. 70 ss. Per una utile sintesi e un aggiornato compendio delle decisioni più significative assunte dalle Autorità domestiche competenti, v. E. Kosta, *Security of Processing and Data Breach Notification*, 18 gennaio 2024.

[3] Sulla risarcibilità dei danni da violazione del GDPR, v. Corte giust., 4 maggio 2023, C-300/21, *UI c. Österreichische Post AG*, con commenti di C. Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, di S. Patti, *Il risarcimento del danno immateriale secondo la Corte di giustizia* e di C. Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, tutti in *Nuova giur. civ. comm*., 2023, rispettivamente a p. 1136 ss., p. 1146 ss., p. 1150 ss.; nonché di A. Palmieri e R. Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, di S. Pagliantini, *Un altro palcoscenico della «guerra» tra le corti: il danno (immateriale) bagatellare dell'art. 82 Gdpr* e di M. Federico, *«La tempesta perfetta»: ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva*, tutti in *Foro it*., 2023, IV, rispettivamente a c. 278 ss., c. 285 ss., c. 293 ss. V., altresì, Cass., 26 aprile 2021, n. 11020, con nota di M. Giraudo, *Responsabilità e danno nel caso di illecito trattamento di dati personali*, in *Nuova giur. civ. comm*., 2021, p. 1074 ss.; Cass., 10 giugno 2021, n. 16402, con nota di M. De Chiara, *L'illecito senza danno e la privacy,* in *Foro it.*, 2021, I, c. 3593 ss. In dottrina, cfr. U. Salanitro, *Illecito trattamento dei dati personali e risarcimento*

 ISBN 978-88-495-5568-4

configura un dovere di mantenimento di un livello di sicurezza adeguato ai rischi, declinato attraverso condotte preventive e reattive. Da un primo e sommario esame del GDPR, oltre a poter censire l'incrementato impatto della *liability rule* e l'affermarsi di un processo di *accountability* – basti pensare alla protezione dei dati *by design* e *by default*, *ex* art. 25 GDPR[4] –, è possibile rilevare una elevazione del livello di protezione dei diritti e delle libertà delle persone fisiche e, quindi, dei soggetti interessati[5].

Giova ricordare come la sicurezza, sin dalla Convenzione di Strasburgo n. 108/81 «Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale», non abbia integrato solamente un canone operativo dell'attività del trattamento dei dati[6], ma sia assurta a principio fondamentale[7]. Ai sensi del testo originario dell'art. 7, «adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate». Anche a seguito delle modifiche apportate alla Convenzione attraverso il Protocollo del Consiglio d'Europa del 17 e 18 maggio 2018, la sicurezza non ha smarrito la sua qualificazione di principio ordinatore[8].

del danno nel prisma della Corte di Giustizia, in *Riv. dir. civ*., 2023, p. 426 ss.; S. Thobani e R. Caterina, *Il diritto al risarcimento dei danni*, in *Giur. it*., 2019, p. 2805 ss.; C. Iorio, *Appunti sulla responsabilità da trattamento dei dati*, in *Actualidad Jurídica Iberoamericana*, 2023, p. 1148 ss. Utili spunti in F. Mezzanotte, *Risk Allocation and Liability Regimes in the IoT*, in A. De Franceschi e R. Schulze (a cura di), *Digital Revolution - New Challenges for Law Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, München, 2019, p. 182 ss. e A.G. Grasso, *GDPR Feasibility and Algorithmic Non-Statutory Discrimination*, Napoli, 2023, p. 89 ss., 107 ss.

[4] Cass., 11 ottobre 2023, n. 28385, in *ilcaso.it*.

[5] Cfr. A. Mantelero e G. Vaciago, *Reconciling Data Protection and Cybersecurity: An Operational Approach for Business Sector*, in R. Senigaglia, C. Irti e A. Bernes (a cura di), *Privacy and Data Protection in Software Services*, eBook, 2022, p. 97 ss.; T. Sica, *Cybersecurity and risk management*, in *Corporate governance*, 2022, p. 581 ss.; P. Laghi, *Struttura della rete e responsabilità: cybersecurity"*, in Aa.Vv., *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020, p. 255 ss.; E. Tosi, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale. Oggettivazione del rischio e riemersione del danno morale con funzione deterrente-sanzionatoria alla luce dell'art. 82 GDPR*, Milano, 2019, spec. p. 73 ss. V., altresì, G. Amore, *Digitalizzazione, protezione dei dati e terzo settore*, in *Juscivile*, 2022, p. 879 ss.

[6] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 81 ss.; Id., *Protezione dei dati e circolazione delle informazioni*, in Id., *Tecnologie e diritti*, Bologna, 1995, p. 41 ss.; V. Frosini, *Diritto alla riservatezza e calcolatori elettronici*, in G. Alpa e M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, Padova, 1984, p. 29 ss.; G. Corasaniti, *Esperienza giuridica e sicurezza informatica*, Milano, 2003.

[7] S. Rodotà, *Tecnologie dell'informazione e frontiere del sistema socio-politico*, in G. Alpa e M. Bessone (a cura di), *Banche dati, telematica e diritti della persona*, cit., p. 89 ss.

[8] Con riguardo alla sicurezza nel trattamento nell'ambito dei sistemi di *National Digi-*

ISBN 978-88-495-5568-4

Tuttavia, la Direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[9], risultò disallineata rispetto alla Convenzione di Strasburgo, in quanto la sicurezza venne degradata a mera regola di condotta, il cui rispetto doveva essere esclusivamente assicurato dal responsabile del trattamento (art. 17)[10]. Veniva prescritta l'adozione di misure tecniche e organizzative appropriate e capaci di assicurare la protezione dei dati personali rispetto a ipotesi di distruzione accidentale o illecita, di perdita accidentale o alterazione, diffusione o accesso non autorizzati, nonché dinanzi al rischio di qualsivoglia forma illecita di trattamento dei dati, con particolare riguardo al trattamento concernente trasmissioni di dati in rete.

Nel testo della l. n. 675/1996, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, la sicurezza non comparve tra le finalità della normativa e, al contempo, non rappresentò un principio per il trattamento dei dati. Tale scelta giuspolitica ebbe una ripercussione a livello di tutela delle posizioni giuridiche soggettive incise dal trattamento dei dati: non fu conferito all'interessato un diritto ad ottenere una tutela anticipatoria, venendo individuato nel solo rimedio risarcitorio lo strumento atto a ricomporre le perdite patite per via della violazione della disciplina della sicurezza[11]. L'adozione di misure di sicurezza era correlata allo stato di conoscenze acquisite in base al progresso tecnico[12]: la custodia e il controllo dei dati, in ragione di ciò, dovevano essere calibrati rispetto alla natura dei dati medesimi e alle specifiche caratteristiche

tal Identity, intesi alla stregua di "*a combination of policy, law, and technology by which a person's personal data are captured to establish and digitally represent, verify and manage a person's legal identity across public (and private) services identified in national policy and law*", v. le *Guidelines on National Digital Identity, The Council of Europe*, 18 novembre 2022, § 3.6.

[9] V. Zeno-Zencovich, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*", in V. Cuffaro, V. Ricciuto e Id. (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 159 ss.

[10] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 809.

[11] Come precisa S. Rodotà, *Elaboratori elettronici e controllo sociale*, cit., p. 92, la tutela risarcitoria risulta(va) successiva e mai pienamente appagante. Per G. Giacobbe, *La responsabilità civile per la gestione di banche dati*, in V. Zeno-Zencovich (a cura di), *Le banche dati in Italia. Realtà normativa e progetti di regolamentazione*, Napoli, 1985, p. 93, la tutela della personalità risulta(va) meglio assicurata mediante rimedi preventivi piuttosto che repressivi. In tema, C. Castronovo, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali* e A. di Majo, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, entrambi in V. Cuffaro, V. Ricciuto e V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, cit., rispettivamente p. 189 ss. e 225 ss.

[12] E. Pellecchia, *La responsabilità civile per trattamento dei dati personali,* in *Resp. civ. e prev*., 2006, p. 226.

 ISBN 978-88-495-5568-4

del trattamento. Inoltre, sorgeva l'obbligo per il titolare del trattamento di adottare misure idonee e preventive, capaci di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati, nonché di accesso non autorizzato o di trattamento non consentito o difforme rispetto alle finalità della raccolta. Il parametro dell'idoneità, tuttavia, impedì un appiattimento del dovere costante di sicurezza sul parametro di quella minima (art. 15, commi 2 e 3, l. n. 675/1996). L'uniformità rispetto alle misure minime di sicurezza, il cui aggiornamento doveva essere biennale, in ragione degli sviluppi tecnici e logistici, non determinava una neutralizzazione del dovere di adottare ogni misura idonea e preventiva[13]: l'osservanza della prima prescrizione non si traduceva in una area di immunità per il titolare del trattamento rispetto a possibili conseguenze in termini di responsabilità civile o amministrativa derivanti dal mancato ricorso ad ogni misura di sicurezza risultata idonea[14].

Il Codice in materia di protezione dei dati personali, d.lgs. n. 196/2003, collocò la sicurezza al Titolo V – Sicurezza dei dati e dei sistemi – del compendio normativo: la previsione di un obbligo di sicurezza (art. 31) ricalcò quanto disposto dal previgente art. 15, comma 1, l. n. 675/1996, mentre furono tenute distinte le misure minime di sicurezza, disciplinate dall'art. 33 e dall'Allegato B del Codice[15].

Con l'entrata in vigore del GDPR, si è assistito ad una espansione della sicurezza, riabilitata a principio del trattamento dei dati personali[16], risultando così centrale nell'incremento della tutela dei diritti e delle libertà delle persone fisiche[17] e, quindi, nella preservazione della componente identitaria[18], specialmente in casi in cui risulti conclamata una situazione

[13] Cfr. S. Rodotà, *Elaboratori elettronici e controllo sociale*, cit., p. 90; G. Conte. *Diritti dell'interessato e obblighi di sicurezza*, in V. Cuffaro e V. Ricciuto (a cura di), *La disciplina del trattamento dei dati personali*, Torino, 1997, p. 264.

[14] S. Sica, Sub *art. 18*, in E. Giannantonio, M.G. Losano e V. Zeno-Zencovich, *La tutela dei dati personali. Commento alla L. 675/1996*, Padova, 1999, p. 254.

[15] Cfr. G.M. Riccio, *Sub artt. 32-36*, in S. Sica e P. Stanzione (a cura di), *La nuova disciplina della privacy. Commento al d.lgs. 30 giugno 2003, n. 196*, Bologna, 2005, p. 126 ss.; R. Motroni, *La sicurezza dei dati e dei sistemi*, in V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *Il Codice del trattamento dei dati personali*, Torino, 2007, p. 221 ss. Per una concreta applicazione, v. il Provvedimento del garante per la protezione dei dati personali del 28 marzo 2019.

[16] Sia consentito un rinvio a M. Renna, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. e prev*., 2020, p. 1343 ss.

[17] E. Lucchini Guastalla, *Privacy e data protection: principi generali*, in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, p. 70; A. Mantelero, *La gestione del rischio*, in G. Finocchiaro (opera diretta da), *La protezione dei dati personali in Italia*, Bologna, 2019, p. 473 ss.

[18] Cfr. G. Resta, *Identità personale e identità digitale*, in *Dir. inf*., 2007, p. 511 ss.; e, ora, G. Guzzardi, *Il paradigma identitario nella società digitale*, in *Persona e mercato*, 2023, p. 525 ss.

ISBN 978-88-495-5568-4

di vulnerabilità[19]: può constatarsi, attraverso la sezione del sito del Garante per la protezione dei dati personali dedicata ai provvedimenti sul *data breach*, come molteplici, ad oggi, risultino essere i fenomeni di violazione dei dati personali in ambito sanitario. I rischi elevati per la tenuta della disponibilità e dell'autenticità dei dati attinenti ad un significativo aspetto della individuale personalità ribadiscono la centralità della protezione capillare dell'identità soggettiva affidata al concorso di tutele privatistiche e pubblicistiche, di rimedi anticipatori e risarcitori e di obblighi legali di protezione[20]. Risulta necessario un impiego costante di apparati tecnici e organizzativi idonei e aggiornati, capaci di minimizzare i rischi e di fornire una reazione subitanea in caso di violazione dei dati personali[21], ovvero, stando al testo dell'art. 4, n. 12, GDPR, di ogni «violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

Il titolare e il responsabile del trattamento sono tenuti a predisporre dispositivi di sicurezza che garantiscano un costante trattamento conforme al GDPR[22], provvedendo al monitoraggio e al governo del *rischio*[23]. Ai sensi dell'art. 32, § 1, GDPR, al fine di assicurare un livello di sicurezza adeguato al rischio, andranno predisposte misure tecniche e organizzative tra cui rientrano: la pseudonimizzazione e la cifratura dei dati personali[24]; la capacità di assicurare permanentemente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; una procedura mediante cui testare, verificare

[19] Cfr. D.J Solove e W. Hartzog, *Breached! Why Data Security Law Fails and How to Improve it*, New York, 2022; R. Sloan e R. Warner, *Why Don't We Defend Better? Data Breaches, Risk Management, and Public Policy*, Boca Raton, FL, 2020.

[20] In tema, F. Zanovello, *Misure di garanzia e rischio di* data breach *in ambito sanitario*, in A. Thiene e S. Corso (a cura di), *La protezione dei dati sanitari.* Privacy *e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, 2023, p. 145 ss.

[21] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 779.

[22] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Torino, 2016, p. 295; A. Mantelero, *La gestione del rischio*, cit., p. 493.

[23] Per alcune considerazioni critiche sul rapporto tra rischio e pericolo, v. S. Sica, Sub *art. 82 GDPR*, in Aa.Vv., *Codice della privacy e data protection*, Milano, 2021, p. 894. V., altresì, M. Gambini, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018, p. 92 ss.

[24] G. Giannone Codiglione, Risk-based approach *e trattamento dei dati personali*, in S. Sica, V. D'Antonio e G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Assago, 2016, p. 67. Per un'applicazione concreta v. il Provvedimento del Garante della protezione dei dati personali del 27 aprile 2023.

 ISBN 978-88-495-5568-4

e valutare regolarmente l'efficacia dei dispositivi tecnici e organizzativi[25]. Tuttavia, come recentemente chiarito dal Garante per la protezione dei dati personali, "gli obblighi di sicurezza imposti dal Regolamento richiedono l'adozione di rigorose misure tecniche e organizzative, includendo, oltre a quelle espressamente individuate dall'art. 32, § 1, lett. da *a*) a *d*), tutte quelle necessarie ad attenuare i rischi che i trattamenti presentano"[26].

La valutazione dell'adeguatezza del livello di sicurezza risulterà condizionata anche dal peso attribuito al rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati (art. 32, § 2, GDPR)[27].

Si fa spazio una visione strategica e globale della sicurezza[28]: la declinazione del principio di sicurezza non tollera una lettura di retroguardia che individui, ancora, nella responsabilità civile il solo strumento di reazione, ma incide e modula in ogni fase – preventiva, operativa e reattiva – l'operato del titolare e del responsabile del trattamento[29].

2. Gli artt. 33 e 34 del GDPR, rispettivamente rubricati «Notifica di una violazione dei dati personali all'autorità di controllo» e «Comunicazione di una violazione dei dati personali all'interessato», *codificano* una gestione trasparente e condivisa dei fenomeni di *data breach*[30].

Il dovere di notifica di una violazione dei dati personali all'autorità di controllo è posto in capo al titolare del trattamento: pur delineandosi un obbligo strettamente personale, la posizione del titolare del trattamento non è irrelata, in quanto, il responsabile del trattamento è tenuto ad informare il titolare senza ingiustificato ritardo dopo aver appreso della vio-

[25] G. Fonderico, *La regolazione amministrativa del trattamento dei dati personali*, in *Giorn. dir. amm*., 2018, p. 420.

[26] Provvedimento del 28 settembre 2023.

[27] In tema, cfr. J. Hladjk, Sub *art. 32 GDPR*, in E. Ehmann e M. Selmayr (a cura di), *Datenschutz-Grundverordnung Beck-LexisNexis*, München, 2018, p. 517 s.; C. Piltz, Sub *art. 32 GDPR*, in *DS-GVO. Kommentar*, in P. Gola e D. Heckmann, München, 2022, p. 664 ss.

[28] G. Resta, *I dati e le informazioni*, in G. Alpa e Id., *Le persone fisiche e i diritti della personalità*, in *Tratt. dir. civ. Sacco*, 1, *Le persone e la famiglia*, Torino, 2019, p. 460, insiste sul carattere preventivo che connota il dovere del titolare del trattamento.

[29] Cfr. C. Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali,* in *Juscivile*, 2020, spec. p. 791 ss.; A. Mollo, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 255 ss.

[30] Per una analisi esauriente, cfr. A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, in *DIMT*, 9 luglio 2018, p. 1 ss.; G. Colacino, *Il danno da trattamento dei dati personali nel GDPR,* in *Rass. dir. civ*., 2023, p. 48 ss. Sia consentito un rinvio a M. Renna, *Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi*, in *Dir. merc. ass. e fin*., 2020, p. 197 ss.

ISBN 978-88-495-5568-4

lazione in essere (art. 33, § 2, GDPR)[31]. Tale prescrizione notiziale, che comprova la pervasività del principio di sicurezza e integra un precipitato dell'*accountability approach*[32], non troverà applicazione qualora il titolare del trattamento riesca a dimostrare l'*improbabilità* di un rischio per i diritti e le libertà delle persone fisiche[33]. Il dovere di notifica di una violazione risulta funzionale alla tutela dell'integrità dei dati e della salvaguardia dei diritti e delle libertà delle persone fisiche ed è fondato sulla procedimentalizzazione della gestione del rischio, nonché modellato in base alla natura e alla gravità della violazione dei dati personali e dei tipi di rischio per l'interessato[34].

A livello operativo, la notifica andrà effettuata entro 72 ore dalla cognizione del *data breach*[35]: il rispetto della tempistica condurrà, allora, il titolare del trattamento a dotarsi di una struttura tecnica, di cui è parte anche il responsabile del trattamento, che favorisca un flusso costante di informazioni e che permetta di apprezzare puntualmente le criticità e di valutare con esattezza la natura dei rischi[36]. Ai sensi dell'art. 33, § 3, GDPR, il titolare dovrà *almeno*:

a) descrivere la natura della violazione dei dati personali, compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

L'obbligo informativo potrà anche essere assolto per fasi: in questo caso,

[31] Cfr. S. Sica, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?*, in Id., V. D'Antonio e G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, cit., p. 8; F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 804.

[32] S. Vigliar, Data breach *e sicurezza informatica*, in S. Sica, V. D'Antonio e G.M. Riccio (a cura di), *La nuova disciplina europea della privacy,* cit., p. 245 ss.; E. Maio, Sub *art. 24 GDPR*, in A. Barba e S. Pagliantini (a cura di), *Delle persone,* II, in *Comm. cod. civ. Gabrielli*, Milano, 2019, p. 503 ss.

[33] La notifica all'autorità di garanzia di una violazione dei dati personali avviene mediante una procedura telematica disponibile al sito servizi.gpdp.it.

[34] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016, p. 291, nt. 54.

[35] P. Voigt e A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide*, eBook, 2017, p. 65 ss.

[36] C. Burton, Sub *art. 33*, in Aa.Vv., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, 2020, p. 640 ss.

 ISBN 978-88-495-5568-4

spetta al titolare del trattamento giustificare le ragioni di una notifica parziale e avviare, contestualmente, un contatto immediato con l'autorità di garanzia. Inoltre, il titolare del trattamento è tenuto a documentare le violazioni dei dati personali, nonché i provvedimenti assunti per porvi rimedio[37].

L'art. 34 GDPR enuclea una serie di regole poste a salvaguardia dei diritti del soggetto interessato in caso di violazione dei dati personali: la comunicazione è legata alla stima del livello di rischio. Solo in caso di rischi *elevati* per i diritti e le libertà delle persone fisiche si procederà in tal senso[38]. Attraverso la comunicazione all'interessato, che dovrà essere fornita mediante un linguaggio chiaro e semplice, si devono trasmettere informazioni essenziali circa lo stato dei dati personali trattati, favorendo una tempestiva reazione da parte dell'interessato. Il titolare del trattamento dovrà rendere edotto l'interessato delle informazioni e delle misure, di cui all'art. 33, § 3, lett. *b*), *c*) e *d*).

Si tratta, nel complesso, di una previsione regolamentare elastica, ma comunque incentrata sull'esigenza di una comunicazione esaustiva e differenziata, là dove ciò risulti necessario al fine della protezione degli interessati[39]. Infatti, ai sensi dell'art. 34, § 3, GDPR, non si ricorrerà a tale comunicazione qualora sia stato approntato uno dei seguenti rimedi[40]:

a) messa in atto di misure tecniche e organizzative adeguate di protezione e contestuale applicazione ai dati personali oggetto della violazione: vi rientrano, in particolare, quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) adozione da parte del titolare del trattamento di misure volte a scongiurare il sopravvenire di un rischio elevato per i diritti e le libertà degli interessati;

c) comunicazione pubblica, o in misura equipollente, che consenta una efficace informazione degli interessati nel caso in cui la diretta comunicazione richieda sforzi sproporzionati[41].

[37] G. Finocchiaro, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, p. 246 s.

[38] V. Zeno-Zencovich, *Liability for data loss*, in V. Mak, E. Tjong Tjin Tai e A. Berlee (a cura di), *Handbook in Data Science and Law*, Cheltenham, 2018, p. 51.

[39] Per un'applicazione concreta, v. il Provvedimento del Garante per la protezione dei dati personali del 14 maggio 2020.

[40] A.G. Parisi, *Illiceità del trattamento dei dati personali e rimedi (inibitori, risarcitori, satisfattivi e ablativi)*, in P. Stanzione (a cura di), *I "poteri privati" e le nuove frontiere della privacy*, Torino, 2022, pp. 225-226.

[41] Per un'applicazione concreta, v. il Provvedimento del Garante per la protezione dei dati personali dell'8 giugno 2023; nonché, il Provvedimento del Garante per la protezione dei dati personali del 10 marzo 2022.

ISBN 978-88-495-5568-4

3. Le linee guida adottate il 28 marzo 2023 provvedono ad aggiornare le precedenti *Guidelines on Personal data breach notification under Regulation 2016/679*, WP250rev.01, del 3 ottobre 2017. L'odierno testo offre una consolidazione di *best practices* in materia di doveri informativi ricadenti sul titolare del trattamento: dalla lettura delle linee guida emerge la conferma di una visione elastica della sicurezza, contestuale e procedimentale, nonché inidonea ad essere *catturata* da schemi regolatori rigidi[42]. Il livello di rischio per i diritti e le libertà delle persone fisiche è centrale per l'effettuazione della notifica e ciò si riflette in termini di necessaria e puntuale pianificazione delle fasi attinenti al *data processing*. Vi rientra l'adeguata professionalizzazione dei soggetti coinvolti nel trattamento, al fine di favorire una immediata cognizione e una pronta e proporzionata reazione a seguito del verificarsi di fenomeni di *data breach*.

La notifica risulterà efficace, e come tale funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, qualora sia tempestiva e circostanziata: ciò implica uno scambio di informazioni tra titolare del trattamento, responsabile del medesimo e responsabile della protezione dei dati personali (ove presente). Il responsabile del trattamento, del caso, dovrà comunicare al titolare l'avvenuta violazione dei dati personali senza indebito ritardo, mettendo a disposizione del titolare ogni informazione che risulti utile al fine della decisione di notificare o meno la violazione dei dati personali. Il responsabile della protezione dei dati ha il dovere di informare il titolare e il responsabile del trattamento e di fornire loro consulenza, oltre a cooperare con l'autorità di controllo e fungere da punto di contatto con riferimento ad ogni questione connessa all'attività del trattamento dei dati.

La notifica potrà essere omessa qualora il titolare del trattamento, dopo aver constatato la consistenza e l'impatto della violazione, reputi *improbabile* una lesione per i diritti e le libertà delle persone fisiche: centrale, ancora una volta, risulta essere l'attività di *risk assessment*[43]. Seguendo le linee guida, dovrà procedersi ad un esame dei rischi collegato ai seguenti fattori: *a*) tipo di violazione; *b*) natura, carattere sensibile e volume dei dati personali; *c*) facilità di identificazione delle persone; *d*) gravità delle conseguenze per le persone fisiche; *e*) caratteristiche particolari dell'interessato; *f*) caratteristiche particolari del titolare del trattamento di dati; *g*) numero di persone fisiche interessate.

Con riguardo alla comunicazione di un fenomeno di *data breach* all'interessato, le linee guida chiariscono come questo strumento notiziale sia

[42] M.S. Esposito, Sub *art. 32 GDPR*, in Aa.Vv., *Codice della privacy e data protection*, cit., pp. 503-505.

[43] A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, cit., p. 14.

 ISBN 978-88-495-5568-4

teso alla salvaguardia effettiva dell'interessato in caso di violazioni dei dati personali che presentino rischi *elevati* in termini di diritti e di libertà personali; la comunicazione dovrà essere diretta, chiara e trasparente e soddisfare il requisito di speditezza. Per il titolare del trattamento diviene, nuovamente, essenziale, al fine di non incorrere in responsabilità di marca aquiliana o amministrativa, dotarsi di un apparato di sicurezza efficiente che consenta l'attivazione dei meccanismi di allerta e che favorisca una reazione proporzionata e capace di mitigare le conseguenze dannose derivanti da violazioni della riservatezza ovvero dell'integrità o della disponibilità dei dati[44].

Una preziosa fonte di orientamento per i soggetti coinvolti nel trattamento è costituita dalle linee guida 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali, adottate dall'EDPB in data 14 dicembre 2021. Per i casi di *ransomware*, di attacchi di esfiltrazione dei dati, di errore umano, di smarrimento o furto di dispositivi o di documenti cartacei, nonché per errato invio di corrispondenza e altri casi, il *board* europeo offre indicazioni precise e un valido supporto d'ausilio per il titolare del trattamento nella valutazione della violazione dei dati concretamente occorsa. Il documento conferma la necessità di una perdurante responsabilizzazione dei soggetti coinvolti nell'attività di trattamento dei dati, rimarcando la centralità della prevenzione e della minimizzazione dell'impatto del *data breach*. Secondo le linee guida, ogni titolare e ogni responsabile del trattamento dovrebbero disporre di piani e procedure per la gestione di violazioni dei dati, stabilendo un netto riparto dei compiti interno e individuando le figure responsabili delle fasi del processo di recupero[45]. In nome del principio di *accountability* e in omaggio alla protezione dei dati fin dalla progettazione, viene caldeggiata la preparazione di un manuale per la gestione delle violazioni dei dati, predisposto dal titolare e dal responsabile del trattamento.

4. Il principio di sicurezza rende evidente la necessità di assicurare un trattamento costantemente capace di proteggere i diritti e le libertà fondamentali delle persone fisiche[46].

[44] A. Mantelero, *La gestione del rischio*, cit., p. 485 ss.

[45] In tema, con riferimento alla formazione di un *Incident Response Team* e alla redazione di una Matrice RACI, volta a "mettere in relazione le risorse con le attività delle quali sono responsabili, o con le loro aggregazioni", v. G. Vaciago, Sub *art. 33 GDPR*, in Aa.Vv, *Codice della* privacy *e* data protection, cit., pp. 518-519. Precisa l'A. che «le risorse vengono distinte in: (i) *Responsible* (colui che esegue ed assegna l'attività); (ii) *Accountable*: è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri 3 ruoli, per ciascuna attività deve essere univocamente assegnato; (iii) *Consulted* è la persona che aiuta e collabora con il Responsible per l'esecuzione dell'attività; (iv) *Informed* è colui che deve essere informato al momento dell'esecuzione dell'attività» (p. 519).

[46] Sui diritti dell'interessato disciplinati dal GDPR, cfr. F. Piraino, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it*., 2019,

ISBN 978-88-495-5568-4

Le prescrizioni comunicative addossate in capo al titolare del trattamento in caso di *data breach* si inseriscono in questo scenario e favoriscono l'affermarsi di una tutela anticipatoria[47]; peraltro, un trattamento conforme alle procedure informative, quand'anche accompagnato dall'adesione ad un codice di condotta (art. 40, § 2, lett. *h* e *i*, GDPR) o dotato di una certificazione (art. 42 GDPR), pur non potendo escludere l'eventuale configurarsi di una responsabilità civile in capo al titolare o al responsabile del trattamento, specialmente quando questi omettano di adottare le misure di sicurezza calibrate sui rischi specifici o non aggiornino i dispositivi di sicurezza[48], potrà incidere sulla quantificazione della sanzione amministrativa pecuniaria inflitta ai sensi dell'art. 83, § 2, lett. *j*), GDPR[49].

Dalla lettura degli artt. 32, 33 e 34 GDPR emerge il delinearsi di un autonomo diritto degli interessati a un trattamento sicuro che conforma in ogni fase l'attività di *data processing*. La predisposizione di meccanismi di sicurezza sempre adeguati e idonei diviene, allora, per il titolare del trattamento un *asset* strategico[50] e ciò richiama l'opportunità di far ricorso

p. 2789 ss.; G. Di Lorenzo, *Spunti di riflessione su taluni «diritti dell'interessato»*, in N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 237 ss.

[47] Chiarisce A. Mantelero, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence"*, in Id. e D. Poletti (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, eBook, 2018, p. 305, che «la sicurezza non è più la mera sicurezza informatica o la sicurezza del processo di trattamento dati, ma è la sicurezza che deriva dalla garanzia del rispetto dei diritti e delle libertà fondamentali. Solo in questa maniera il primato dell'Unione Europea nel regolare il trattamento dei dati personali potrà rimanere tale, mantenendo fermo un paradigma valoriale, in cui la tutela dei diritti e libertà dei singoli e della collettività prevale su modelli di innovazione dominati dalle dinamiche di mercato».

[48] G.M. Riccio e F. Pezza, *Certification mechanisms and liability rules under the GDPR. When the harmonisation becomes unification*, in A. De Franceschi e R. Schulze (a cura di), *Digital Revolution - New Challenges for Law Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies*, cit., p. 150.

[49] V. Considerando 81 GDPR. Si configura una mera presunzione di adeguamento al GDPR che permette un'attenuazione dell'onere della prova in capo al titolare e al responsabile del trattamento, nel caso in cui vengano chiamati a rispondere per danni derivanti dall'attività di trattamento dei dati personali. In tema, D. Poletti e M.C. Causarano, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, cit., p. 379; S. Calzolaio, L. Ferola, V. Fiorillo, E.A. Rossi e M. Timiani, *La responsabilità e la sicurezza del trattamento*, in L. Califano e C. Colapietro (a cura di), *Innovazione tecnologica e valore della persona - Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 169. Per alcune considerazioni critiche, v. N. Maccabiani, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Oss. fonti*, 2022, 3, p. 77.

[50] F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, cit., p. 782. Ora, L. Miotto, *Organizzazione d'impresa e gestione dei dati personali. Il rischio di non compliance nelle catene di fornitura*, Torino, 2023, spec. p. 44 ss.

 ISBN 978-88-495-5568-4

ad appositi meccanismi assicurativi[51] che si rivelino capaci di assorbire le esternalità negative derivanti da un'eventuale responsabilità per danni causalmente connessi alla violazione delle previsioni regolamentari in materia di sicurezza[52], senza che ciò intacchi il regime di responsabilità amministrativa delineato dall'art. 83 GDPR[53].

[51] V. il documento redatto da IVASS, Indagine sulle polizze a copertura del cyber risk, ottobre 2023. In tema, J. Wolff, *Cyberinsurance policy. Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks*, Cambridge, Massachusetts, 2022, spec. p. 65 ss. Sia consentito un rinvio a M. Renna, *Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi*, cit., p. 218 ss.

[52] Con riferimento al rapporto tra *accountability* e responsabilità civile, chiarisce G. Comandè, *Lettera sulla responsabilità (civile) e l'autonomia (individuale)*, in *Danno e resp*., 2022, p. 668: «Così sono i meccanismi e le prassi caratteristici dell'attività e largamente lasciati all'autonomia del singolo a divenire parametro per verificare se le scelte di autonomia organizzativa per prevenire o per come reagire a un data breach conducano o meno a responsabilità o si fermino a rendicontare tempestivamente le azioni a tutela poste in essere, per esempio. In tal modo, anche la causazione di un danno non porta automaticamente a risarcirlo se si sono rispettati i parametri e le modalità comportamentali previste dal sistema; viceversa, anche la mancata causazione di un danno risarcibile può portare ad una "sanzione" per la "mera" violazione della *accountability*». In tema, A. Spangaro, *Il* data breach *tra obblighi di notifica e principio di autoresponsabilità*, cit., p. 26 ss.

[53] F. Mezzanotte, *L'allocazione convenzionale del rischio «da illecito» (con particolare riguardo alle sanzioni amministrative pecuniarie)*, in *Riv. dir. civ*., 2010, II, p. 203 ss. Cfr., altresì, S. Landini, *Assicurazione e responsabilità*, Milano, 2004, p. 343 ss.; C.F. Giampaolino, *Le assicurazioni. L'impresa - I contratti*, in *Tratt. dir. comm. Buonocore*, III, Torino, 2013, p. 182 ss.

ISBN 978-88-495-5568-4

Tommaso Mauceri

Quale futuro per l'identità digitale. Rilievi conclusivi.

Ringrazio Gaetano Guzzardi di avermi reso partecipe di questa iniziativa consentendomi così di arricchirmi, grazie all'ascolto di contributi così interessanti, su una tematica tra le più urgenti ed attuali.

Agli inizi degli anni duemila v'è stato un interessantissimo dibattito sugli scambi senza accordo che ha in qualche modo contribuito a preservare e consegnare al nuovo secolo un (sia pur essenziale) principio di consensualità che deve necessariamente governare l'ambito contrattuale e con esso il mondo degli scambi; come risulta anche dalla contestuale circostanza che, sia in Italia che in Europa, è proseguita la legislazione volta a rendere più chiari e trasparenti i modelli di contrattazione con i consumatori.

Adesso, però, il problema è diverso, come ben evidenzia, sul piano del linguaggio, il passaggio dal paradosso degli «scambi senza accordo» alla dittatura dei «mercati senza scambio».

L'oggetto assai ambito di questi nuovi mercati, pur nella disparità dei vari, singoli aspetti e prodotti specifici, è ben noto e riguarda il vastissimo fenomeno delle informazioni digitali in grado di incidere sui modelli di consumo connessi a: abitudini delle persone, ideali, valori, gusti e desideri di ogni genere, abilità, aspirazioni, costumi, *modus vivendi*, mezzi di comunicazione e trasporto utilizzati; tutto ciò che può essere disseminato e di cui può restare traccia nel *mare magnum* del web ovvero del *cloud*, in una battuta, «il petrolio del terzo millennio». E già, perché ogni informazione in qualsiasi modo connessa ai modelli di consumo rappresenta un valore aziendale, un risparmio sui costi di produzione, a volte addirittura un bene a sé autonomamente cedibile a terzi a titolo oneroso. Ecco perché tali utilità vengono appropriate in nuovi regni digitali di proprietà privata.

Cos'è che preoccupa maggiormente? Cos'è che fa avvertire questo mercato come particolarmente pericoloso, come un attentato agli equilibri democratici che il mondo occidentale ha con fatica guadagnato nella storia recente e perfino ai modelli di definizione della identità umana?

Anche il dibattito di questo pomeriggio testimonia che gli aspetti problematici son plurimi e complessi però vorrei accennare, in queste considerazioni riassuntive a tre aspetti principali sui quali, non a caso, hanno particolarmente insistito le relazioni che mi hanno preceduto e che, sia pure a costo di un eccesso di semplificazione, potremmo sinteticamente enunciare nei seguenti termini: a) anticoncorrenzialità del mercato; b) impossibilità

 ISBN 978-88-495-5568-4

di una contrattazione reale; c) imperscrutabilità (non sottoponibilità a controllo) degli *output* e connessi rischi di manipolazione della persona.

Il primo punto, relativo al carattere anticoncorrenziale del mercato c.d. *big tech*, è stato ampiamente chiarito nella relazione di Gaetano Guzzardi (e v. *supra Tutela della persona e sviluppo tecnologico nella società dell'informazione*) nell'apprezzabile tentativo di valorizzare tutti gli strumenti, analiticamente illustrati, della normativa europea per la tenuta del sistema democratico comunque ritenuti comunque, in definitiva, «insufficienti e inadeguati». Quanto ai pericoli, basti qui accennare allo strapotere economico (che si traduce in una situazione di vero e proprio oligopolio) delle c.dd. *mag-seven* e cioè delle ben note Alphabet-Google, Amazon, Apple, Meta-Facebook e Microsoft (c.dd. *big five*) alle quali vanno aggiunte Nvidia, al primo posto nella produzione di microprocessori, e Tesla, non certo per l'aspetto del trasporto ma per l'accesso senza precedenti a informazioni digitali obbligatoriamente fornite per l'utilizzo stesso del veicolo dai propri utenti. Basta guardare i dati relativi a queste imprese (offerti ad esempio da *companiesmarketcap.com*) per rendersi conto di come la ricchezza rappresentata dai dati digitali tende a concentrarsi nella sfera di un numero limitato di operatori che viene ad assumere un ruolo nel mercato finora inconcepibile.

Il secondo punto, relativo alla difficoltà di un consenso (e corrispettivamente di una revoca) di natura adeguata e consapevole, è forse l'aspetto che più avvicina il nostro tema alla teoria del contratto e che, però, al contempo, ne profila le incolmabili distanze che, infatti, hanno portato la dottrina a parlare di mercato senza scambi. Infatti, e al di là dei tentativi più o meno felici della normativa (soprattutto europea) di sottoporre a controllo prassi commerciali di appropriazione arbitraria dei dati personali mediante la valorizzazione del consenso, della relativa revoca e/o rettifica/integrazione e la posizione del principio di sicurezza resta il fatto che non sempre è chiaro il bene, il «prodotto digitale» per l'ottenimento del quale il consenso viene prestato; ancora, non è agevole comprendere nemmeno a cosa si presta il consenso, alla cessione di quali beni, al tipo di utilizzo che poi ne verrà fatto. Non sappiamo di quale aspetto della nostra identità personale si approprierà di fatto l'impresa della *big tech* che stiamo autorizzando né è detto che noi verremo mai realmente a conoscenza di quel nostro aspetto. Con riferimento allo strumento della revoca del consenso, poi, al di là delle difficoltà pratiche connesse al relativo esercizio, va notato che non sempre esso pare realmente prestarsi a una tutela effettiva, soprattutto quando il dato, aggregato ad altri, è ormai entrato a far parte di nuovi beni. Del resto, fin quando non riceve una segnalazione specifica, come impone la normativa di sicurezza illustrataci da Mario Renna (*supra*, *L'identità sicura: il banco di prova del* data breach), il consumatore non è consapevole di eventuali abusi o c.dd. *data breach*. Proprio l'idea di Renna di meccanismi

ISBN 978-88-495-5568-4

assicurativi in favore del titolare o del responsabile del trattamento, del resto, è condivisibile in quanto in linea con le accorte strategie dell'operatore di mercato, ma può finire per rendere più difficile l'ingresso di nuovi concorrenti e, di riflesso, ancor meno protetta la posizione del consumatore, attenuandosi la valenza deterrente.

Sul terzo punto, relativo all'imperscrutabilità degli *output* e al rischio di manipolazione della persona mi paiono condivisibili le preoccupazioni di Emanuele Tuccari sulle difficoltà di stabilire confini netti tra accettabili (purché trasparenti) sistemi di IA finalizzati all'inferenza di intenzioni o emozioni umane funzionali a un mercato efficiente e casi di inaccettabile manipolazione della volontà di persone o gruppi di persone, specie se vulnerabili (*supra*, *Note minime sull'asistematica disciplina del neuromarketing*). Desidero anche richiamarmi, tra i tanti studi sull'argomento (celebratissimo, ad esempio, *Il capitalismo della sorveglianza* della Zuboff), a un recentissimo libro di Yanis Varoufakis dal titolo assai eloquente "*Tecnofeudalesimo. Cosa ha ucciso il capitalismo*" (pubblicato proprio in questi giorni nella traduzione italiana di Salvatore Serù da La nave di Teseo, 2023). Nel rappresentare in modo semplice e lineare la storia del capitalismo (p. 92 ss.), l'A. a un certo punto osserva che gli algoritmi con i quali le imprese della *big tech* processano i nostri dati, non svolgono più un ruolo passivo ma «si sono trasformati in agenti» comportandosi come finora hanno sempre fatto le persone e incidendo in modo significativo sui loro modelli di comportamento e sui modelli di costruzione della loro identità (specialmente, p. 115). Così, ad esempio, una volta che abbiamo fornito all'algoritmo che orienta Alexa alcuni dati salienti sulle nostre abitudini e i nostri desideri «Alexa inizia a istruire noi. (…). Comincia con delle leggere esortazioni a fornirle maggiori informazioni… che poi personalizza in accessi a video, testi e musica che apprezziamo» (p. 101) innescandosi un circolo vizioso nel quale noi siamo sempre più sensibili alle sollecitazioni di Alexa. Se ciò può destare alcune perplessità al cospetto di persone in età adulta deve procurare un gravissimo allarme quando in ballo ci sono giovani vite, la loro conformabilità a modelli consumistici ben calibrati e, in qualche modo, il futuro stesso dell'umanità. Col rischio, in definitiva, che nella replica dei modelli algoritmici e spersonalizzanti sfioriscano le qualità che da sempre hanno contraddistinto l'attività umana che sono legate al mondo delle emozioni e consistono soprattutto nella creatività, nel pensiero originalmente analogico senza il quale non si sarebbero ottenuti tanti progressi scientifici.

Ecco perché dà una grande consolazione e un messaggio di speranza la testimonianza così seria dell'impegno di giovani studiosi in tematiche così attuali e urgenti per un diritto più giusto e una società più umana.

 ISBN 978-88-495-5568-4

Gli Autori

Gaetano Guzzardi, *Ricercatore di Diritto privato, Università degli Studi di Catania*

Giuseppe Marino, *Ricercatore di Diritto privato, Università degli Studi di Palermo*

Tommaso Mauceri, *Professore associato di Diritto privato, Università degli Studi di Catania*

Mario Renna, *Ricercatore di Diritto privato, Università degli Studi di Siena*

Alessandro Scuderi, *Professore associato di Economia ed estimo rurale, Università degli Studi di Catania*

Emanuele Tuccari, *Ricercatore di Diritto privato, Università degli Studi di Pavia*

Giuseppe Versaci, *Ricercatore di Diritto privato, Università degli Studi dell'Insubria*

Mariangela Ziccardi, *Ricercatrice di Diritto privato, Università degli Studi del Molise*

 ISBN 978-88-495-5568-4

Per i tipi Giuffrè

1. A. Coniglio, *Osservazioni al progetto preliminare del codice di procedura civile* (esaurito).
2. C. Sanfilippo, *Pauli Decretorum Libri Tres* (1938), (esaurito).
3. G. Grassetti, R. Nicolò, M. Petroncelli, *Osservazioni e proposte sul progetto del secondo libro del codice civile* (1938), p. 137.
4. M. Scarlata Fazio, *La successione codicillare* (1939), p. 220.
5. M. Giorgianni, *Il negozio d'accertamento* (1939), (esaurito).
6. M. Giorgianni, *Contributo alla teoria dei diritti di godimento su cosa altrui*, I. (1940), (esaurito).
7. G. Astuti, *Studi intorno alla promessa di pagamento. Il costituto di debito*, II. (1941), p. XII, 336.
8. M. Giorgianni, *La dichiarazione di morte presunta* (1943), (esaurito).
9. C. Sanfilippo, Condictio indebiti. - I. *Il fondamento dell'obbligazione da indebito* (1943), p. 98.
10. C. Caristia, *Pietro Giannone "giureconsulto" e "politico". Contributo alla storia del giurisdizionalismo italiano* (1947), p. 148.
11. C. Cosentini, *Studi sui liberti. Contributo allo studio della condizione giuridica dei liberti cittadini*, I. (1948), p. XII, 274.
12. C. Sanfilippo, *Bibliografia romanistica italiana* [1939-1949] (1949), p. 102.
13. G. Catalano, *Le ultime vicende della Legazia apostolica in Sicilia. Dalla controversia liparitana alla legge delle guarentigie* [1711-1871] (1950), p. X, 234.
14. C. Cosentini, *Studi sui liberti. Contributo allo studio della condizione giuridica dei liberti cittadini*, II. (1950), p. 200.
15. S. Di Paola, *Donatio mortis causa*, I. (1952), p. IX, 264.
16. S. Di Paola, *Confessio in iure*, I. (1952), p. IV, 106.
17. C. Cosentini, *Condicio impossibilis* (1952), p. VIII, 208.
18. G. Olivero, *«Dissimulatio» e «tolrantia» nell'ordinamento canonico* (1953), p. 208.
19. C. Caristia, *Scritti giuridici, storici e politici*. I. *Scritti giuridici* (1953), p. VIII, 496.
20. F. La Rosa, *I peculi speciali in diritto romano* (1953), p. 248.
21. A. Pavone, *Il registro delle imprese* (1954), p. XII, 664.
22. S. Di Paola, *Saggi in materia di "hereditatis petitio"* (1954), p. VIII, 124.
23. C. Caristia, *Scritti giuridici, storici e politici*. II. *Scritti storici e politici* (1955), p. VIII, 536.
24. S. Cassarino, *Le situazioni giuridiche e l'oggetto della giurisdizione amministrativa* (1956), p. IV, 416.
25. C. Cosentini, *Miscellanea romanistica* (1956), p. IX, 265.
26. E. Grasso, *L'espropriazione della quota* (1957), p. XXIV, 368.
27. C.M. Bianca, *Il divieto del patto commissorio* (1957), p. VIII, 360.
28. F. Leonardi, *Introduzione allo studio del comportamento sociale* (1958) (esaurito).
29. F. Durante, *Ricorsi individuali ad organi internazionali* (1958), p. VIII, 176.
30. F. Finocchiaro, *Uguaglianza giuridica e fattore religioso* (1958), p. VIII, 328.
31. C. Sapienza, *Conversione e consecuzione dei procedimenti concorsuali* (1958), p. VII, 224.
32. D. Siracusano, *Studio sulla prova delle esimenti* (1959), p. IV, 248.
33. S. Puleo, *I diritti potestativi (individuazione della fattispecie)* (1959), p. IV, 244.
34. R. Provinciali, *Norme di diritto processuale nella costituzione* (1959), p. VIII, 204.

35. F. La Rosa, *Studi sull'«actio iudicati»* (1960), p. IV, 216.
36. M. Condorelli, *I fondamenti giuridici della tolleranza religiosa nell'elaborazione canonistica dei secoli XII-XIV. Contributo storico-dogmatico* (1960), p. IV, 172.
37. S. Cassarino, *La destinazione dei beni degli enti pubblici* (1962), p. IV, 203.
38. G. Nicosia, *L'acquisto del possesso mediante i «potestati subiecti»* (1960), p. XVI, 496.
39. E. Giardina, *Le basi teoriche del principio della capacità contributiva* (1961), p. VIII, 480.
40. C. Lazzara, *Il contratto di locazione* (1961), p. VIII, 260.
41. P. Barcellona, *Profili della teoria dell'errore nel negozio giuridico* (1962), p. IV, 244.
42. I. Andolina, *Profili dogmatici della esecuzione forzata espropriativa*, I. (1962), p. IV, 428.
43. V. Piano Mortari, *L'azione revocatoria nella giurisprudenza medievale* (1962), p. VIII, 232.
44. F. Durante, *L'ordinamento interno delle Nazioni Unite* (1964), p. XLIV, 448.
45. V. Frosini, *La struttura del diritto*, sesta ed. (1977), p. XII, 280.
46. F. La Rosa, *L'«actio iudicati» nel diritto romano classico* (1963), p. IV, 228.
47. C.M. Bianca, *Il debitore e i mutamenti del destinatario del pagamento* (1963), p. VI, 330.
48. F. Finocchiaro, *La «laicità» dello Stato in Francia* (1963), p. VIII, 146.
49. V. Frosini, *La ragione dello Stato* (1963), p. VIII, 184.
50. E. Grasso, *La pronuncia di ufficio*. I. *La pronuncia di merito* (1967), p. VIII, 348.
51. M. Condorelli, *Destinazione di patrimoni e soggettività giuridica nel diritto canonico. Contributo allo studio degli enti non personificati* (1964), p. VIII, 192.
52. N. Salanitro, *L'invalidità delle deliberazioni del consiglio di amministrazione di società per azioni* (1965), p. IV, 264.
53. *Studi in onore di Gaetano Zingali* (1965), 3 Voll.:
    Vol. I. *Economia, finanza e statistica*, p. XVI, 672;
    Vol. II. *Diritto pubblico*, p. IV, 656;
    Vol. III. *Diritto privato e storia del diritto*, p. IV, 664.
54. G. Nicosia, *Studi sulla «deiectio»*, I. (1965), p. 184.
55. P. Barcellona, *Intervento statale e autonomia privata nella disciplina dei rapporti economici* (1969), p. IV, 300.
56. A. Barbera, *I principi costituzionali della libertà personale* (1971), p. IV, 236.
57. A. Vitale, *La dichiarazione del fallimento* (1967), p. VIII, 248.
58. N. Palazzolo, *Dos praelegata. Contributo alla storia del prelegato romano* (1968), p. XII, 256.
59. N. Salanitro, *Gli acquisti del coniuge del fallito* (1969), p. XII, 292.
60. S. La Rosa, *Eguaglianza tributaria ed esenzioni fiscali* (1968), p. IV, 352.
61. O. Condorelli, *Scritti sul diritto e sullo Stato* (1970), p. XXXVI, 576.
62. I. Andolina, *Introduzione alla teoria del titolo esecutivo, Fondamento e limiti del principio* "non est inchoandum ab exsecutione" (1968), p. IV, 176.
63. P. Petino, *Rapporto di amministazione e rapporto di lavoro subordinato* (1968), p. 308.
64. C. Lazzara, *I rapporti agrari consuetudinari in Sicilia nell'attuale momento legislativo* (1969), p. IV, 200.
65. G. Barone, *L'intervento del privato nel procedimento amministrativo* (1969), p. VIII, 272.
66. A. La Pergola, *Residui «contrattualistici» e struttura federale nell'ordinamento degli Stati Uniti* (1969), p. VIII, 456.
67. *Condizioni generali di contratto e tutela del contraente debole*. Tavola rotonda presso l'istituto di Diritto Privato (1970), p. IV, 252.
68. V. Frosini, *Teoremi e problemi di scienza giuridica*, ristampa inalterata (1975), p. VIII, 284.
69. A. Barbera, *Regioni e interesse nazionale*, ristampa inalterata (1974), p. XII, 370.
70. N. Salanitro, *Il fallimento dell'imprenditore defunto* (1974), p. XII, 164.
71. L. Arcidiacono, *Organizzazione pluralistica e strumenti di collegamento* (1974), p. IV, 168.

72. S.E. Battiato, *La tassazione dei trasferimenti della ricchezza a titolo gratuito* (1974), p. IV, 416.
73. G. Lo Castro, *Personalità morale e soggettività giuridica nel diritto canonico* (1974), p. IV, 252.
74. N. Palazzolo, *Potere imperiale ed organi giurisdizionali nel II secolo d. C.* (1974), p. XII, 292.
75. *Studi in memoria di Orazio Condorelli* (1974), 3 Voll.:
    Vol. I. p. VIII, 464.
    Vol. II. p. IV, 465-926.
    Vol. III. p. IV, 927-1408.
76. P. Abbadessa, *La gestione dell'impresa nella Società per azioni* (1975), p. IV, 220.
77. A. Vitale, *I debiti della massa nel fallimento* (1975), p. 204.
78. G. Ziccone, *Le cause «sopravvenute» di non punibilità* (1975), p. 148.
79. E. Sciacca, *Le radici teoriche dell'assolutismo nel pensiero politico francese del primo cinquecento (1498-1519)* (1975), p. VIII, 184.
80. V. Di Cataldo, *Il concordato fallimentare con assunzione* (1976), p. IV, 284.
81. V. Gueli, *Scritti vari* (1976), 2 Voll.:
    Tomo I. p. VIII, 752.
    Tomo II. p. IV, 753-1376.
82. S. Sambataro, *L'abolizione del contenzioso nel sistema di giustizia amministrativa* (1977), p. 292.
83. T.A. Auletta, *Riservatezza e tutela della personalità* (1978), p. IV, 228.
84. F. D'Agostino, *Per un'archeologia del diritto* (1979), p. VIII, 164.
85. V. Di Cataldo, *L'imitazione servile* (1979), p. IV, 228.
86. A. Belfiore, *Interpretazione e dommatica nella teoria dei diritti reali* (1979), p. IV, 620.
87. G. Bivona, *I contratti d'integrazione verticale in agricoltura* (1979), p. IV, 138.
88. M. Barcellona, *Inattuazione dello scambio e sviluppo capitalistico* (1980), p. IV, 248.
89. L. Arcidiacono, *Profili di riforma dell'amministrazione statale* (1980), p. IV, 288.
90. G. Barone, *Aspetti dell'attività interna della pubblica amministrazione* (1980), p. IV, 132.
91. M. Paradiso, *Il danno alla persona* (1981), p. IV, 320.
92. A. D'Atena, *Le Regioni e la Comunità Economica Europea* (1981), p. IV, 136.
93. E. Zappalà, *Il principio di tassatività dei mezzi di prova nel processo penale* (1982), p. VIII, 288.
94. F. D'Agostino, *Diritto e secolarizzazione (Pagine di Filosofia giuridica e politica)* (1982), p. XII, 324.
95. I. Andolina, *Contributo alla dottrina del titolo esecutivo* (1982), p. IV, 140.
96. *Studi in onore di Cesare Sanfilippo* (1982) 7 Voll.:
    Vol. I. p. XII, 768.
    Vol. II. p. IV, 780.
    Vol. III. p. IV, 784.
    Vol. IV. p. IV, 800.
    Vol. V. p. IV, 804.
    Vol. VI. p. IV, 788.
    Vol. VII. p. IV, 812.
97. M. Tedeschi - G. Catalano - P. Bellini - P. Lombardia - E.G. Vitali - M. Condorelli - F. Finocchiaro - L. De Luca, *Storia e dogmatica nella scienza del diritto ecclesiastico* (1982), p. IV, 212.
98. R. Vigo, *Libertà e divieti nella circolazione delle notizie bancarie* (1983), p. IV, 212.
99. R. Maccarrone, *Profili sistematici dell'effetto espansivo esterno della sentenza di riforma* (1983), p. IV, 216.

100. F. D'Agostino, BIA *Violenza e giustizia nella filosofia e nella letteratura della Grecia Antica* (1983), p. XII, 132.
101. S. Pettinato, *«Sollicitudo pro universa ecclesia»* (1983), p. VIII, 180.
102. T.A. Auletta, *Alimenti e solidarietà familiare* (1984), p. VIII, 228.
103. C. Costa, *Il rappresentante comune degli azionisti di risparmio* (1984), p. VIII, 140.
104. M. Paradiso, *La comunità familiare* (1984), p. VIII, 444.
105. L. Ventura, *Il principio di eguaglianza nel diritto del lavoro* (1984), p. IV, 392.
106. S. Amato, *Sessualità e corporeità. I limiti dell'identificazione giuridica* (1985), p. VIII, 228.
107. E.V. Napoli, *L'inabilitazione* (1985), p. XII, 208.
108. E. Zappalà, *L'impugnazione "tardiva" della sentenza penale nella pratica giurisprudenziale* (1985), p. 184.
109. I. Marino, *Servizi pubblici e sistema autonomistico* (1987), ristampa emendata, p. VIII, 300.
110. S. Mangiameli, *La proprietà privata nella Costituzione* (1986), p. IV, 196.
111. B. Caruso, *Contributo allo studio della democrazia nel sindacato*, I, (1986), p. IV, 232.
112. S. Seminara, *Tecniche normative e concorso di persone nel reato* (1987), p. VIII, 448.
113. *L'indirizzo fenomenologico e strutturale nella filosofia del diritto italiana più recente,* a cura di Francesco D'Agostino (1988), p. VIII, 236.
114. A. Ruggeri, *Le attività "conseguenziali" nei rapporti fra la Corte Costituzionale e il legislatore* (1988), p. VIII, 300.
115. *Studi in memoria di Mario Condorelli* (1988) 4 Voll.:
    Vol. I. p. XII, 620.
    Vol. II. p. IV, 668.
    Vol. III. p. VIII, 578.
    Vol. IV. p. VIII, 420.
116. S. Ferlito, *L'attività internazionale della Santa Sede* (1988), p. IV, 204.
117. *Scritti in onore di Giuseppe Auletta* (1988) 3 Voll.:
    Vol. I. p. XVI, 688.
    Vol. II. p. IV, 744.
    Vol. III. p. IV, 708.
118. C. Romeo, *Impresa assistita e diritto del lavoro* (1988), p. IV, 244.
119. F. Musumeci, *Inaedificatio* (1988), p. IV, 240.
120. E. Zappalà, *La ricusazione del giudice penale* (1989), p. 168.
121. S. Aleo, *Il disvalore e le forme generali della responsabilità penale. Prospettive di teoria e riforma del diritto penale* (1989), p. 228.
122. P. Petino, *Composizione delle liti e ruolo del sindacato* (1989), p. 372.
123. T. Auletta, *Il fondo patrimoniale* (1990), p. 380.
124. A. Ruggeri, *Le crisi di governo tra ridefinizione delle regole e rifondazione della politica* (1990), p. 224.
125. C. Turco, *Interesse negativo e responsabilità precontrattuale* (1990), p. 761.
126. R. Sapienza, *Il principio del non intervento negli affari interni* (1990), p. 172.
127. *Studi in onore di Cesare Sanfilippo* (1991), Vol. VIII, p. VIII, 187.
128. A. Cariola, *La nozione costituzionale di pubblico impiego* (1991), p. 280.
129. R. Pennisi, *La convalida del marchio* (1991), p. 204.
130. G. Meliadò, *Il rapporto di lavoro nei gruppi di società. Subordinazione e imprese a struttura complessa* (1991), p. 202.
131. A.C. Amato Mangiameli, *La fondazione delle norme tra decisionismo e cognitivismo nel dibattito tedesco contemporaneo* (1991), p. 164.
132. V.E. Ragusa, *Vizi del processo decisorio nelle formazioni organizzate e diritti dei terzi* (1992), p. VI, 278.

133. V. Ottaviano, *Scritti giuridici* (1992) 3 Voll.:
Vol. I. p. 510.
Vol. II. p. 428.
Vol. III. p. 504.
134. E. Castorina, *Autonomia universitaria e Stato pluralista* (1992), p. 160.
135. S. Muscarà, *Riesame e rinnovazione degli atti nel diritto tributario* (1992), p. 464.
136. A. Costanzo, *Condizioni di incoerenza. Un'analisi dei discorsi giuridici* (1992), p. XX, 248.
137. F. Arcaria, *Senatus censuit. Attività giudiziaria ed attività normativa del Senato in età Imperiale* (1992), p. 352.
138. M. Ricca, *L'abrogazione delle leggi di derivazione concordataria. Profili costituzionali* (1993), p. VIII, 282.
139. A. Cariola, *Referendum abrogativo e giudizio costituzionale. Contributo allo studio di potere sovrano nell'ordinamento pluralista* (1994), p. VIII, 424.
140. C. Paterniti, *La causa del fatto-reato* (1994), p. IV, 140.
141. B. Montanari, *Filosofia del diritto: identità scientifica e didattica, oggi* (1994), p. X, 148.
142. I. Nicotra Guerrera, *Territorio e circolazione delle persone nell'ordinamento costituzionale* (1995), p. VI, 228.
143. F. Santangeli, *L'interpretazione della sentenza civile* (1996), p. VI, 492.
144. M. Meli, *Il principio comunitario "chi inquina paga"* (1996), p. IV, 202.
145. T. Rafaraci, *Le nuove contestazioni nel processo penale* (1996), p. VIII, 540.
146. R. Sapienza, *Dichiarazioni interpretative unilaterali e trattati internazionali* (1996), p. X, 292.
147. M. Condorelli, *Scritti di storia e di diritto* (1996), p. LXVIII, 672.
148. C. Camardi, *Economie individuali e connessione contrattuale. Saggio sulla presupposizione* (1997), p. VI, 526.
149. M. Cavallaro, *Il regime di separazione dei beni fra i coniugi* (1997), p. VI, 200.
150. M.R. Maugeri, *Violazione delle norme contro l'inquinamento ambientale e tutela inibitoria* (1997), p. VI, 324.

Nuova Serie

151. G. Ragusa Maggiore, *Scritti giuridici* (1997) 3 Voll.:
Vol. I. p. X, 514.
Vol. II. p. X, 515-1034.
Vol. III. p. X, 1535-1561.
152. G. Mineo, *Il finanziamento agevolato tra legge e contratto* (1997), p. VI, 264.
153. G. Di Rosa, *Rappresentanza e gestione. Forma giuridica e realtà economica* (1997), p. VI, 312.
154. I. Nicotra Guerrera, *"Vita" e sistema dei valori nella Costituzione* (1997), p. VI, 234.
155. E. Castorina, *Introduzione allo studio della cittadinanza. Profili ricostruttivi di un diritto* (1997), p. VI, 309.
156. E. Grasso, *Le leggi, la dottrina e la giurisprudenza* su *I Processi Civili nell'ultimo cinquantennio* (1998) 3 Voll.:
Vol. I. p. XV, 524.
Vol. II. p. VIII, 525-1115.
Vol. III. p. VIII, 1117-1650.
157. *Trans-National Aspects of Procedural Law*, X World Congress on Procedural Law a cura di Italo Andolina-Taormina 17-23 settembre 1995 (1998) 3 Voll.:
Vol. I. p. X, 484.
Vol. II. p. X, 485-846.
Vol. III. p. X, 845-1247.

158. *La dottrina giuridica italiana alla fine del XX secolo. Un bilancio* a cura di Bruno Montanari (1998), p. IV, 177.
159. A. Alaimo, *La partecipazione azionaria dei lavoratori. Retribuzione, rischio e controllo* (1998), p. XI, 236.
160. S. Randazzo, *'Leges Mancipii'. Contributo allo studio dei limiti di rilevanza dell'accordo negli atti formali di alienazione* (1998), p. IV, 192.
161. F. Migliorino, *Misterya concursus. Itinerari premoderni del diritto commerciale* (1999), p. VI, 204.
162. M. Genovese, *Gli interventi edittali di Verre in materia di decime sicule* (1999), p. VI, 496.
163. V. Patanè, *L'individualizzazione del processo penale minorile. Confronto con il sistema inglese* (1999), p. IV, 215.
164. *Scritti in onore di Antonio Pavone La Rosa* (1999):
    Vol. I. *Saggi di diritto commerciale* - tomo 1, p. XXIV, 484.
    Vol. I. *Saggi di diritto commerciale* - tomo 2, p. X, 485-982.
    Vol. I. *Saggi di diritto commerciale* - tomo 3, p. X, 983-1496.
    Vol. II. *Saggi vari*, p. X, 1497-2114.
165. L. Lombardo, *La prova giudiziale. Contributo alla teoria del giudizio di fatto nel processo* (1999), p. XIV-622.
166. A. Giussani, *Le dichiarazioni di rinuncia nel giudizio di cognizione* (1999), p. VI, 186.
167. A. Lo Faro, *Funzioni e finzioni della contrattazione collettiva comunitaria. La contrattazione collettiva come risorsa dell'ordinamento giuridico comunitario* (1999), p. VI, 354.
168. *L'esame e la partecipazione a distanza nei processi di criminalità organizzata,* a cura di Enzo Zappalà (1999), p. IV, 282.
169. M. D'Antona, *Opere*, a cura di Bruno Caruso e Silvana Sciarra (2000):
    Vol. I. *Scritti sul metodo e sulla evoluzione del diritto del lavoro - Scritti sul diritto del lavoro comparato e comunitario*, p. XVIII, 452.
    Vol. II. *Scritti sul diritto sindacale*, p. VI, 450.
    Vol. III. *Scritti sul diritto del lavoro*:
    tomo 1, p. VI, 1-462.
    tomo 2, p. VI, 463-936.
    tomo 3, p. VI, 937-1300.
    Vol. IV. *Scritti sul pubblico impiego e sulla pubblica amministrazione*, p. VI, 304.
    Vol. V. *Recensioni, note ed altri scritti*, p. VIII, 452.
170. A. Ciancio, *Il reato ministeriale. Percorsi di depoliticizzazione* (2000), p. VIII, 352.
171. *Biotecnologie. Profili scientifici e giuridico-sociali.* Atti del Convegno, Catania - Villa Cerami, 28 maggio 1999, a cura di Bruno Montanari (2000), p. IV, 158.
172. F. Arcaria, *Referre ad principem. Contributo allo studio delle epistulae imperiali in età classica* (2000), p. X, 320.
173. G. Auletta, *Scritti giuridici* (2001) 8 Voll.:
    Vol. I. p. 526.
    Vol. II. p. 534.
    Vol. III. p. 496.
    Vol. IV. p. 538.
    Vol. V. p. 562.
    Vol. VI. p. 554.
    Vol. VII. p. 548.
    Vol. VIII. p. 542.
174. A.M. Maugeri, *Le moderne sanzioni patrimoniali tra funzionalità e garantismo* (2001), p. XVIII, 974.

175. G. Speciale, *Antologia giuridica. Laboratori e rifondazioni di fine Ottocento* (2001), p. VI, 224.
176. M. Meli, *Autonomia privata, sistema delle invalidità e disciplina delle intese anticoncorrenziali* (2001), p. X, 198.
177. F. Santangeli, *L'ordinanza successiva alla chiusura dell'istruzione* (2001), p. X, 484.
178. A. Grasso, *Illiceità penale e invalidità del contratto* (2002), p. VIII, 108.
179. F. Giuffrè, *La solidarietà nell'ordinamento costituzionale* (2002), p. X, 388.
180. C.M. Bianca, *Realtà sociale ed effettività della norma. Scritti giuridici* (2002):
Vol. I. *Teoria generale e fonti - Persone e famiglia - Garanzie e diritti reali*:
tomo 1, p. XII, 628.
tomo 2, p. IV, 629-1210.
Vol. II. *Obbligazioni e contratti - Responsabilità*:
tomo 1, p. XII, 474.
tomo 2, p. IV, 475-990.
181. G. Di Rosa, *Proprietà e contratto. Saggio sulla multiproprietà* (2002), p. VIII, 284.
182. A. Andronico, *La decostruzione come metodo. Riflessi di Derrida nella teoria del diritto* (2002), p. XIV, 194.
183. B. Troncarelli, *Complessità e diritto. Oltre la ragione sistemica* (2002), p. XII, 214.
184. R. Calisti, *Il sospetto di reati. Profili costituzionali e prospettive attuali* (2003), p. X, 426.
185. U.A. Salanitro, *Contratti onerosi con prestazione incerta* (2003), p. X, 356.
186. M.R. Maugeri, *Abuso di dipendenza economica e autonomia privata* (2003), p. X, 224.
187. M. Paradiso, *I contratti di gioco e scommessa* (2003), p. X, 336.
188. G. Raiti, *La collaborazione giudiziaria nell'esperienza del rinvio pregiudiziale comunitario* (2003), p. X, 534.
189. S. Longo, *Filius familias se obligat? Il problema della capacità patrimoniale dei filii familias* (2003), p. VIII, 328.
190. *Politica comunitaria di coesione economica e sociale e programmazione economica regionale,* a cura di Rosario Sapienza (2003), p. VI, 168.
191. E. Palazzolo, *Ordinamento costituzionale e formazione dei trattati internazionali* (2003), p. XVI, 430.
192. F. Romeo, *La tutela del "consumatore" nel contratto di assicurazione danni* (2004), p. XII, 230.
193. *L'armonizzazione del diritto privato europeo. Il piano d'azione 2003*, a cura di Marisa Meli - Maria Rosaria Maugeri (2004), p. X, 400.
194. B. Spampinato, *L'interesse a ricorrere nel processo amministrativo* (2004), p. XII, 236.
195. P. Pirrone, *L'obbligo di conformarsi alle sentenze della Corte Europea dei Diritti dell'Uomo* (2004), p. VIII, 284.
196. G. Chiara, *Titolarità del voto e fondamenti costituzionali di libertà ed eguaglianza* (2004), p. X, 284.
197. B. Troncarelli, *Logica della globalizzazione e diritto* (2004), p. XII, 130.
198. *Labour law and flexibility in Europe. The cases of Germany and Italy,* a cura di B. Caruso - M. Fuchs (2004), p. 254.
199. G. Messina, *Contraddizioni e aporie dell'universalismo giuridico contemporaneo* (2004), p. VIII, 238.
200. A. Puleo, *Quale giustizia per i diritti di libertà? Diritti fondamentali, effettività delle garanzie giurisdizionali e tecniche di tutela inibitoria* (2005), p. VI, 432.
201. C. Marino, *La delibazione delle sentenze ecclesiastiche di nullità matrimoniale nel sistema italiano di diritto internazionale privato e processuale* (2005), p. XII, 386.
202. *I mobili confini dell'autonomia privata,* a cura di Massimo Paradiso (2005), p. VI, 864.

203. N. Salanitro, *Profili sistematici della società a responsabilità limitata* (2005), p. X, 120.
204. G. Ricci, *Tempi di lavoro e tempi sociali. Profili di regolazione giuridica nel diritto interno e dell'UE* (2005), p. XX, 556.
205. R. Sicurella, *Diritto penale e competenze dell'Unione Europea. Linee guida di un sistema integrato di tutela dei beni giuridici sovrannazionali e dei beni giuridici di interesse comune* (2005), p. X, 658.
206. *Dove va la giustizia penale minorile? Confronto tra l'esperienza francese e i progetti di riforma italiani,* a cura di Enzo Zappalà (2005), p. XX, 218.
207. A. Andronico, *La disfunzione del sistema. Giustizia, alterità e giudizio in Jacques Derrida* (2006), p. XIV, 244.
208. *Studi in onore di Cesare Massimo Bianca* (2006):
    Tomo I, p. XII, 668.
    Tomo II, p. VI, 800.
    Tomo III, p. VI, 1098.
    Tomo IV, p. VI, 946.
209. *Scienza tecnologia & diritto (ST&D)*. Atti del Convegno, Catania-Villa Cerami, 30 maggio 2003, a cura di Bruno Montanari (2006), p. XVI, 104.
210. S. Figuera, *Sul carattere monetario dell'economia capitalistica. Smith, Ricardo, Marx e la teoria neoclassica della moneta* (2006), p. XII, 246.
211. A. Lo Giudice, *Il soggetto plurale. Regolazione sociale e mediazione simbolica* (2006), p. XIV, 332.
212. I. Zingales, *Pubblica amministrazione e limiti della giurisdizione tra principi costituzionali e strumenti processuali* (2007), p. XIV, 298.
213. *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia*. Atti del Convegno, Catania, Villa Cerami, 9-11 giugno 2005, a cura di Tommaso Rafaraci (2007), p. XII, 740.
214. *Studi per Giovanni Nicosia* (2007):
    Tomo I, p. XII, 538.
    Tomo II, p. VI, 558.
    Tomo III, p. VI, 510.
    Tomo IV, p. VI, 546.
    Tomo V, p. VI, 534.
    Tomo VI, p. VI, 530.
    Tomo VII, p. VI, 544.
    Tomo VIII, p. VI, 572.
    Indici, p. IV, 188 (*per i tipi Giappichelli*).
215. *Bilanci e prospettive del diritto di famiglia a trent'anni dalla riforma,* a cura di Tommaso Auletta (2007), p. VIII, 474.
216. F. Leotta, *La competenza legislativa nei sistemi autonomisti. Dalla crisi della sovranità statale all'affermarsi della sussidiarietà* (2007), p. X, 354.
217. *La tutela internazionale dei beni culturali nei conflitti armati,* a cura di Paolo Benvenuti - Rosario Sapienza (2007), p. XII, 382.
218. A.M. Maugeri, *La responsabilità da comando nello statuto della Corte Penale Internazionale* (2007), p. XII, 844.
219. S.A. Cristaldi, *Il contenuto dell'obbligazione del venditore nel pensiero dei giuristi dell'età imperiale* (2007), p. X, 314.
220. *Verso un nuovo processo penale. Opinioni a confronto sul progetto di riforma Dalia*. Atti del Convegno di studi, Catania, Villa Cerami, 18-19 novembre 2005, a cura di Angelo Pennisi (2008), p. VIII, 526.
221. *Le sanzioni patrimoniali come moderno strumento di lotta contro il crimine: reciproco*

riconoscimento e prospettive di armonizzazione, a cura di Anna Maria Maugeri (2008), p. VI, 582.

222. M. Barcellona, *Il danno non patrimoniale* (2008), p. VIII, 136.
223. A. Ciancio, *I gruppi parlamentari. Studio intorno a una manifestazione del pluralismo politico* (2008), p. X, 348.
224. A.M. Maugeri, *La tutela dei beni culturali nel diritto internazionale penale. Crimini di guerra e crimini contro l'umanità* (2008), p. VIII, 352.
225. *Rileggere Keynes. La lezione di John Maynard Keynes a 70 anni dalla pubblicazione della Teoria generale*, a cura di Maurizio Caserta - Stefano Figuera (2008), p. VIII, 176.
226. *Le fonti private del diritto commerciale*, a cura di Vincenzo Di Cataldo - Pierpaolo M. Sanfilippo (2008), p. VI, 467.
227. R. Sicurella, *Per una teoria della colpevolezza nel sistema dello Statuto della Corte Penale Internazionale* (2008), p. VIII, 490.

Per i tipi Giappichelli

228. *Il tempo e il processo.* Scritti scelti di Italo Andolina, a cura di Giovanni Raiti (2009), 2 Voll. indivisibili:
    Vol. I. p. XIV, 458.
    Vol. II. p. VI, 459-889.
229. F. Arcaria, *Diritto e processo penale in età augustea. Le origini della cognitio criminale senatoria* (2009), p. VIII, 164.
230. A. Bettetini, *L'errore in diritto canonico* (2009), p. VIII, 226.
231. A. Las Casas, *Tutele dell'investimento precontrattuale e razionalità economica. Profili comparatistici* (2009), p. XII, 466.
232. V. Scalia, *Profili penalistici e obblighi di tutela nella giurisprudenza della camera dei diritti dell'uomo per la Bosnia e l'Erzegovina*. (2009), p. XIV, 264.
233. R. Sorice, *"… quae omnia bonus iudex considerabit…"* La giustizia criminale nel Regno di Sicilia (secolo XVI) (2010), p. VIII, 200.
234. R. Cavallo, *L'antiformalismo nella temperie weimariana* (2009), p. VIII, 178.
235. B. Spampinato, *Tipologia degli interessi legittimi e forme di tutela* (2010), p. XII, 150.
236. *Où va la justice pénale des mineurs?* (Allemagne, Espagne, France, Italie, Russie), a cura di Sylvie Cimamonti, Gaëtan di Marino, Enzo Zappalà (2010), p. VI, 286.
237. *Il pensiero giuridico di Francesco Santoro Passarelli. Giornata di studio in memoria*, a cura di Bruno Montanari (2010), p. VI, 112.
238. *Il danno ambientale tra prevenzione e riparazione.* Atti del Convegno di studi, a cura di Ida Nicotra e Ugo Sala- nitro (2010), p. VIII, 268.
239. *Studi in onore di Luigi Arcidiacono* (2010):
    Vol. I. p. XL, 1-492.
    Vol. II. p. VIII, 493-994.
    Vol. III. p. VIII, 995-1508.
    Vol. IV. p. VIII, 1509-2012.
    Vol. V. p. VIII, 2013-2530.
    Vol. VI. p. VIII, 2531-3050.
    Vol. VII. p. VIII, 3051-3498.
240. *Liberty and Language. The global dimension of European constitutional integration,* a cura di Emilio Castorina e Pasquale Policastro (2010), p. VI, 490.
241. A. Lo Giudice, *Istituire il postnazionale. Identità europea e legittimazione* (2011), p. XIII, 314.

242. M.S. Testuzza, *Tra cielo e terra. I congegni dell'obbedienza medievale* (2011), p. VI, 188.
243. F. Cristofari, *Chiavi di lettura del principio famiglia e identità di genere* (2011), p. X, 142.
244. *La Convenzione Europea dei diritti dell'uomo e il giudice italiano*, a cura di Francesco Salerno e Rosario Sapienza (2011), p. XII, 177.
245. A. Vitale, *I poteri delle parti nel vecchio impianto del fallimento. Il modello originario di processo fallimentare tra mercato ed economia mista: ragioni di una crisi* (2011), p. VIII, 156.
246. *Temi di ricerca per la tutela dei diritti umani* (2011), a cura di Vincenzo Di Cataldo e Vania Patanè, p. VIII, 490.
247. *Il potere delle immagini. Tecnologia, spazi urbani e luoghi politici* (2011), a cura di Bruno Montanari e Alessio Lo Giudice, p. VIII, 200.
248. *Circolazione dei valori giuridici e tutela dei diritti e delle libertà fondamentali,* a cura di Pasquale Pirrone (2011), p. X, 238.
249. T. Cavallaro, *Il novum probatorio nel giudizio di revisione* (2011), p. XIV, 234.
250. C.M. Pettinato, *I "Maestri di Würzburg" e la costruzione del Jus Publicum Ecclesiasticum nel secolo XVIII* (2011), p. X, 302.
251. *L'Unione Europea dopo il Trattato di Lisbona. Atti del Convegno* (2011), a cura di Nicoletta Parisi e Valentina Petralia, p. VIII, 352.
252. S. La Rosa, *Scritti scelti* (2011):
    Vol. I. p. X, 1-362.
    Vol. II. p. VI, 363-822.
    Vol. III. p. VI, 823-1096.
253. M. Genovese, *Mortis causa capitur. Di una speciale categoria di acquisti patrimoniali* (2011), p. X, 296.
254. G. Nicosia, *Dirigenze responsabili e responsabilità dirigenziali pubbliche* (2011), p. XIV, 244.
255. S. Longo, *Senatusconsultum Macedonianum. Interpretazione e applicazione da Vespasiano a Giustiniano* (2012), p. XII, 280.
256. F. Paterniti, *Legislatori regionali e Legislazione europea. Le prospettive delle Regioni italiane nella fase ascendente di formazione del diritto dell'Unione europea dopo il Trattato di Lisbona* (2012), p. VIII, 270.
257. E. Bivona, *Certificazione di qualità dei prodotti e tutele civilistiche* (2012), p. X, 248.
258. G. Majorana, *Il patto fra generazioni negli ordinamenti giuridici contemporanei. Dallo sviluppo sostenibile all'equilibrio finanziario: la necessità di un lungimirante rapporto fra generazioni* (2012), p. VIII, 271.
259. A. Consoli, *Giurisdizione penale ed efficienza. Procure della Repubblica tra vincoli e produttività* (2012), p. XIV, 134.
260. D. Messineo, *La garanzia del "contenuto essenziale" dei diritti fondamentali. Dalla tutela della dignità umana ai livelli essenziali delle prestazioni* (2012), p. VIII, 336.
261. F. Giuffrè, *Unità della Repubblica e distribuzione delle competenze nell'evoluzione del regionalismo italiano* (2012), p. VIII, 177.
262. A. Zappulla, *La formazione della notizia di reato. Condizioni, poteri ed effetti* (2012), p. X, 410.
263. R. La Rosa, *Ricerche sul quasi usufrutto nel diritto romano* (2012), p. X, 194.
264. *Il pluralismo alla prova dei nuovi mezzi di comunicazione*, a cura di Adriana Ciancio (2012), p. VIII, 176.
265. G.A. Ferro, *Modelli processuali ed istruttoria nei giudizi di legittimità costituzionale* (2012), p. XII, 342.
266. *Il controllo penale dell'immigrazione irregolare: esigenze di tutela, tentazioni simboliche, imperativi garantistici*, a cura di Rosaria Sicurella (2012), p. XIV, 391.

267. *La costruzione dell'identità europea: sicurezza collettiva, libertà individuali e modelli di regolazione sociale*, a cura di Bruno Montanari (2012):
Tomo I. p. XIV, 1-454.
Tomo II. p. XII, 1-462 (2013).
268. F. Musumeci, *Protezione pretoria dei minori di 25 anni e ius controversum in età imperiale* (2013), p. XII, 262.
269. *La responsabilità sociale dell'impresa. In ricordo di Giuseppe Auletta*, a cura di V. Di Cataldo e P.M. Sanfilippo (2013), p. VI, 135.
270. T. Mauceri, *Enti collettivi e danno non patrimoniale* (2013), p. X, 188.
271. C. Benanti, *Scioglimento della comunione legale e disciplina del patrimonio* (2013), p. VIII, 350.
272. G. Vitale, *Principi generali e diritto derivato. Contributo allo studio del sistema delle fonti dell'Unione europea* (2013), p. X, 150.
273. P. Sciuto, *Concetti giuridici e categorie assiomatiche: l'uso di rescindere nell'esperienza di Roma antica* (2013), p. X, 304.
274. S. Bosa, *Atti della vita quotidiana e tutela civile dell'incapace* (2013), p. X, 162.
275. T. Mauceri, *Sponsorizzazione e attività sportiva* (2014), p. VIII, 210.
276. *Un diritto senza terra? Funzioni e limiti del principio di territorialità nel diritto internazionale e dell'Unione europea / A Lackland Law? Territory, Effectiveness and Jurisdiction in International and EU Law*, a cura di Adriana Di Stefano (2015), 2 Voll. indivisibili:
Vol. I. p. XXII, 1-322.
Vol. II. p. VIII, 323-782.
277. V. Papa, *Attività sindacale delle organizzazioni datoriali* (2017), p. XIV, 234.
278. D. Arcidiacono, *Parassitismo e imitazione servile non confusoria* (2017), p. X, 254.
279. A.G. Lanzafame, *La* vis expansiva *della rappresentanza. Forme di governo, vocazione presidenziale, resistenze costituzionali* (2019), p. X, 374.
280. R. Belfiore, *Il sequestro preventivo. Tra esigenze impeditive e strumentalità alla confisca* (2019), p. XII, 308.
281. G. Guzzardi, *La permuta atipica. Tratti ricostruttivi e regole operazionali* (2019), p. XVIII, 310.
282. *Ripensare o "rinnovare" le formazioni sociali? Legislatori e giudici di fronte alle sfide del pluralismo sociale nelle democrazie contemporanee*, a cura di A. Ciancio (2020), p. XII, 356.
283. E. Mottese, *La lotta contro il danneggiamento e il traffico illecito di beni culturali nel diritto internazionale. La Convenzione di Nicosia del Consiglio d'Europa* (2020), p. XXII, 218.
284. M. Militello, *Conciliare vita e lavoro. Strategie e tecniche di regolazione* (2020), p. XVI, 256.
285. I. Spadaro, *Il contrasto allo* hate speech *nell'ordinamento costituzionale globalizzato* (2020), p. XVIII, 398.
286. *Specialità delle giurisdizioni ed effettività delle tutele*, a cura di A. Guidara (2021), p. XXXII, 816.
287. G. Galluccio, *Persona giuridica amministratore e società di capitali. Profili di disciplina* (2021), p. VIII, 264.
288. C. Costa, A. Mirone, R. Pennisi, P.M. Sanfilippo, R. Vigo (a cura di), *Studi di diritto commerciale per Vincenzo Di Cataldo* (2021)
Vol. I. *Proprietà intellettuale e concorrenza*, p. XXVI-662.
Vol. II. *Impresa, Società, Crisi d'impresa*.
Tomo I. p. XII-516.
Tomo II. p. IV-1040.

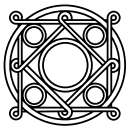
289. G. Di Rosa, S. Longo, T. Mauceri (a cura di), *Percorsi interdisciplinari in tema di rapporto obbligatorio. Atti delle giornate di studi (Catania, 10 ottobre 2019 - 9 luglio 2020 - 1 e 22 marzo 2021)* (2021), p. XII-308.
290. A.G. Grasso, *Maternità surrogata altruistica e tecniche di costituzione dello status* (2022), p. XVI-312.
291. M. Cavallaro, F. Romeo, E. Bivona, M. Lazzara (a cura di), *Sui mobili confini del diritto. Tra pluralità delle fonti ufficiali e moltiplicarsi di formanti normativi "di fatto"* (2021)
    Vol. I. I Sessione: *Persone e famiglia* - II Sessione: *Proprietà*, p. XIV-562.
    Vol. II. III Sessione: *Responsabilità* - IV Sessione: *Contratto*, p. X IV-690.
292. C. Vasta, *Delibere assembleari "collegate" nella società per azioni* (2022), pp. VIII-216.
293. D. Arcidiacono, *La tutela dei marchi che godono di rinomanza. "Al di là del rischio di confusione"* (2022), pp. XIV-466.
294. S. La Rosa, *Altri scritti scelti* (2023), pp. XII-300.
295. *Realtà sociale ed effettività della norma* (in corso di pubblicazione)

Per i tipi Edizioni Scientifiche Italiane

296. G. Di Rosa, S. Longo, T. Mauceri (a cura di), *Diritto e tecnologia. Precedenti storici e problematiche attuali.* Atti delle giornate di studi (Catania, 8 ottobre 2021 - 21 e 22 ottobre 2022 - 25 novembre 2022 - 19 e 20 maggio 2023), 2024, pp. 316.

LA BUONA STAMPA

Questo volume è stato impresso
nel mese di maggio dell'anno 2024 per
la Edizioni Scientifiche Italiane S.p.a.
Stampato in Italia



Edizioni Scientifiche Italiane

www.edizioniesi.it info@edizioniesi.it

https://www.edizioniesi.it
https://www.esidigita.it
edizioni_scientifiche_italiane
Edizioni Scientifiche Italiane
Edizioni Scientifiche Italiane