LUISS

Dipartimento
di Giurisprudenza

Cattedra European private law

Tutela dei dati personali e antitrust: il caso dei sistemi IoT alla luce della sentenza Facebook/Germany (Bundeskartellamt B6-22/16)

Prof. Pierluigi Congedo
RELATORE

Prof. Francesco Ricci
CORRELATORE

Elena Mandarà matr. 142023
CANDIDATO

Anno Accademico 2020/2021

INDICE

Abbreviazione	Spiegazione
AGCM	Autorità Garante della Concorrenza e del Mercato
AGCOM	Autorità Garante delle Comunicazioni
AgID	Agenzia per l'Italia Digitale
AI	Intelligenza Artificiale
API	Application Programming Interfaces
App	Application
Art. 29 WP	Article 29 Working Party
B2B	Business to business
BaaS	Blokchain-as-a-service
CGUE	Corte di Giustizia dell'Unione Europea
CNIL	Commission nationale de l'informatique et des libertés
CoE	Council of Europe
DAO	Decentralized autonomous organization
DDDC	Digital Democracy and Data Commons
DLT	Distributed Ledger Technology
DO	Decentralized organization
DPIA	Data Protection Impact Assessment
EC - Commissione	Commissione Europea
ECHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Innovation Security
EPRS	European Parliamentary Research Service
FRA	European Union Agency for Fundamental Rights
FTC	Federal Trade Commission
GAFAM	Google, Amazon, Facebook, Apple, Microsoft
GDPR	Regolamento (UE) 2016/679
GPDP	Autorità Garante per la protezione dei dati personali
GWB	Das Gesetz gegen Wettbewerbsbeschränkungen
ICO	Information Commissioner's Office
IoT	Internet of things
IP	Proprietà Intellettuale
KYC	Know Your Customer
OECD	Organization for Economic Coperation and Development
PETs	Privacy-Enhancing Technologies
SEP	Standard Essential Patents
TFUE	Trattato sul Funzionamento dell'Unione Europea
UE	Unione Europea
VPN	Virtual Private Network

PRESENTAZIONE

L'economia moderna viene generalmente definita *"data-driven"*, ossia basata sui dati.

I Big Data – le enormi quantità di dati prodotti, scambiati e analizzati mediante sofisticate tecniche algoritmiche – hanno anzitutto rivoluzionato i modelli di *business* adottati dalle imprese, nonché la struttura dei mercati su cui queste operano (cosiddetti mercati "multilaterali"). Le grandi piattaforme digitali ad oggi dominanti sul mercato (Google, Amazon, Facebook, Apple e Microsoft - da qui in poi "GAFAM") hanno infatti intuito e sfruttato il valore economico dei dati, derivante dalle informazioni che è possibile trarne e che consentono alle imprese di adeguare l'offerta alle preferenze e alle necessità dei consumatori. In questo contesto, i dati personali hanno assunto un valore inestimabile, che si scontra con gli standard di tutela degli individui disposti dalla disciplina dell'Unione Europea (da qui in poi "UE").

L'indagine svolta muove dalla considerazione che la disciplina concorrenziale vigente non abbia adeguatamente tenuto conto del crescente valore economico assunto dai dati ed in particolare dei dati personali, ossia quelli che, ai sensi del Regolamento (UE) 2016/679 (d'ora in poi "GDPR"), consentono l'identificazione del soggetto interessato. Il valore economico dei dati, infatti, è strettamente correlato alle informazioni che è possibile trarne e mediante le quali le imprese sono in grado di fornire beni e servizi in grado di soddisfare in modo sempre più "personale" gli utenti finali, poiché basati sullo studio e l'analisi delle preferenze manifestate da questi ultimi.

L'applicazione della disciplina dettata dal GDPR, volta a tutelare il soggetto interessato riconoscendogli il pieno controllo sui propri dati personali, ne limita però lo sfruttamento da parte delle imprese. I rischi per i dati personali crescono insieme allo sviluppo delle nuove tecnologie – come sistemi *Internet of things* (d'ora in poi "IoT"), la *blockchain*, gli *smart contract* e l'Intelligenza Artificiale (d'ora in poi "AI") – il cui funzionamento è prevalentemente basato sull'analisi algoritmica dei dati e sull'utilizzo dei risultati ottenuti nella definizione dei beni e servizi offerti.

E' proprio in questo contesto che si inserisce il presente lavoro, con il quale s'intende dimostrare che l'utilizzo congiunto di queste diverse tecnologie e lo sviluppo di soluzioni innovative sul piano tecnico oltre che normativo non soltanto avrebbe un impatto positivo sulle prestazioni, ma garantirebbe soprattutto una maggiore tutela dei dati personali, riducendo al contempo i rischi per la concorrenza.

Il primo capitolo si apre con una disamina dei nuovi *business* model adottati dalle imprese e delle caratteristiche proprie dei mercati digitali, mettendo in luce in che modo la disciplina concorrenziale attualmente vigente non sia stata in grado di intercettare per tempo i cambiamenti che stavano avvenendo sul mercato, mancando di riconoscere ai dati il ruolo di vero e proprio *asset* strategico che questi hanno assunto. Limitando le proprie valutazioni ai soli elementi di natura strettamente economica

tradizionalmente tenuti in considerazione, le autorità nazionali competenti per la concorrenza negli Stati Membri e la stessa Commissione Europea (d'ora in poi "Commissione"), non sono state in grado di frenare l'ascesa delle grandi piattaforme, né di prevenirne o bloccarne comportamenti abusivi e potenzialmente distorsivi degli equilibri di mercato. L'elemento principale che occorre qui mettere in luce riguarda il fenomeno della cosiddetta "competizione sulla privacy", con il quale si fa riferimento al fatto che, considerato il valore economico assunto dai dati personali, la capacità delle imprese di eludere la disciplina posta a tutela di questi ultimi si traduce in vantaggio competitivo e, a determinate condizioni, può addirittura costituire un abuso di posizione dominante.

Il fatto che l'utilizzo dei dati ponga al contempo dei rischi sia per la concorrenza che per la tutela dei dati personali suggerirebbe la necessità di un'applicazione conforme, se non addirittura congiunta, delle normative che regolano l'uno e l'altro settore. Dall'analisi della principale giurisprudenza dell'UE su questo profilo è emerso però il limite consistente proprio nell'avere sempre tenuto l'una e l'altra volutamente distinte. Tale scelta si basa sul presupposto che, mentre il diritto alla concorrenza persegue il fine di tutelare le imprese che operano sul mercato, la disciplina sulla tutela dei dati è ispirata alla volontà di tutelare i singoli individui.

In virtù della diversa *ratio* da cui muovono, si è dunque sempre giustificata l'assoluta separazione dei rispettivi ambiti di applicazione. In questo contesto si colloca la decisione assunta dal *Bundeskartellamt* – l'Autorità tedesca competente per la concorrenza - nella pronuncia risalente a febbraio 2019[1] contro Facebook. L'illustrazione del caso in questione mira ad evidenziare il rivoluzionario principio ivi affermato, ossia che la violazione della disciplina sulla tutela dei dati personali possa costituire al tempo stesso una violazione della disciplina sulla concorrenza. Sebbene il caso sia stato deciso sulla base della legislazione tedesca, di recente riformata proprio al fine di adeguare quest'ultima alle peculiarità dei mercati digitali, questa nuova apertura potrebbe avere degli effetti rilevanti anche a livello europeo, specialmente alla luce delle recenti proposte di riforma presentate dalla Commissione.

Nel dicembre 2020, la Commissione ha infatti presentato due importanti proposte di Regolamento – il Digital Market Act[2] e il Digital Service Act[3] – che, congiuntamente, costituiscono il Digital Market Package. Lo scopo di questi provvedimenti è proprio quello di riformare la disciplina sulla concorrenza, riducendo il potere di mercato delle piattaforme e ponendo le imprese di dimensioni più piccole nelle condizioni di competere equamente con queste ultime. Per raggiungere questi obiettivi, le proposte di

[1] Bundeskartellamt (2019) B6-22/16 *Facebook, exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing*.

[2] Commissione Europea, "Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)" COM(2020) 842 final, accessibile da https://eur-lex.europa.eu/legal-content/it/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN.

[3] Commissione Europea, "Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE" COM(2020)725, accessibile da https://eur-lex.europa.eu/legal-content/it/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN.

Regolamento introducono una serie di obblighi in capo ai cosiddetti *"gatekeeper"*, identificati essenzialmente sulla base di criteri dimensionali. Tali obblighi riguardano prevalentemente la condivisione dei dati e tengono conto delle condizioni particolari a cui è soggetto il trattamento dei dati personali, a dimostrazione del fatto che la Commissione abbia bene intuito il gap che affligge la disciplina vigente.

La convergenza fra la tutela dei dati personali e la disciplina sulla concorrenza è confermata da altri due importanti fattori. In primo luogo, nell'ambito del proprio piano di riforme la Commissione ha mutuato dalla disciplina dettata dal GDPR alcuni elementi caratteristici, come il diritto alla portabilità dei dati, al fine di migliorare la disciplina concorrenziale vigente. In secondo luogo, le proposte di Regolamento muovono verso un ribaltamento dell'approccio *ex post* e di tipo rimediale prevalentemente adottato da quest'ultima, favorendo invece un intervento *ex ante*, che riduca a monte la possibilità di possibili rischi. Questo aspetto rileva in quanto si tratta del medesimo approccio adottato proprio nell'ambito della tutela dei dati personali e favorito dal fatto che in quel caso sia in gioco la tutela di diritti fondamentali dell'individuo.

Questo approccio si riflette particolarmente nel cosiddetto principio di *privacy-by-design*, in virtù del quale è incoraggiata l'adozione, già in fase di progettazione, di soluzioni tecniche che garantiscano il rispetto della disciplina.

Queste prospettive di riforma si inseriscono nel contesto di un più ampio progetto, in cui rientrano ulteriori proposte quali quelle concernenti l'adozione di una normativa europea, auspicabilmente di rango regolamentare, volta a disciplinare l'utilizzo dell'Intelligenza Artificiale[4] e quelle volte a trasformare l'attuale Direttiva e-Privacy[5] (avente ad oggetto l'utilizzo dei dati personali nelle telecomunicazioni) in Regolamento, al fine di garantirne un'applicazione uniforme su tutto il territorio UE. Si tratta dell'approdo di un percorso già intrapreso nel 2018 con l'adozione del GDPR, che dimostra la strenua volontà da parte dell'UE non soltanto di favorire le imprese che operano nel mercato interno, adeguando la legislazione al progresso tecnologico, ma anche di far sì che lo sviluppo avvenga comunque nell'assoluto rispetto dei diritti fondamentali e garantisca la tutela dei singoli individui. Il capitolo include dunque un'attenta analisi del GDPR alla luce delle problematiche poste dall'avvento dei Big Data.

Il secondo capitolo muove dallo studio dei sistemi IoT, dei quali si è voluto illustrare in primo luogo la natura, il funzionamento e le potenziali applicazioni, per poi soffermarsi sulla disamina dei rischi e degli aspetti problematici legati non soltanto alla tutela dei dati personali, ma anche della concorrenza.

[4] Commissione Europea, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final.
[5] Direttiva del Parlamento Europeo e del Consiglio 2002/58/EC del 12 Luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata del settore delle comunicazioni elettroniche [2002] OJ L. 201/37.

L'analisi muove da alcune riflessioni sulla compatibilità dei suddetti sistemi rispetto alla disciplina del GDPR, evidenziando le difficoltà poste dalla difficile distinzione fra dati e dati personali e dall'inadeguatezza di alcuni concetti chiave ivi contenuti, come ad esempio la nozione di soggetto interessato, che non consente di tutelare i rischi in cui incorre il singolo in quanto membro di un determinato gruppo e non individualmente considerato.

L'approccio che si è inteso seguire è volto a dimostrare che tali problematiche possono essere risolte – o quantomeno tenute maggiormente sotto controllo – attraverso lo sviluppo di soluzioni tecniche e innovative, basate sull'integrazione di tecnologie diverse. Questo non soltanto per ovviare al problema della naturale obsolescenza della legge a cui si assiste sempre più di frequente, ma anche per favorire la convergenza fra discipline diverse garantendone il rispetto per così dire "strutturalmente". Quanto più si rafforzerà il legame fra diritto alla concorrenza e tutela dei dati, tanto più sarà necessario per le imprese che intendono investire nell'impiego delle nuove tecnologie assicurarsi di avere a disposizione strumenti che non si pongano in contrasto con i princìpi dettati da queste ultime. Quanto più le due discipline convergeranno verso un'evoluzione coerente ed omogenea, tanto più sarà semplice intraprendere questa direzione.

Questo presupposto è il filo conduttore dell'intera analisi, che prosegue volgendo l'attenzione verso le possibili violazioni in ambito concorrenziale. Posto che le ipotesi prese in considerazione sono tutte basate sullo sfruttamento economico dei dati, la loro rilevanza in questa sede discende prevalentemente dalla considerazione che, proprio grazie all'utilizzo degli algoritmi, la linea di demarcazione fra dati personali e no è sempre più sottile ed è difficile valutare in quali circostante la violazione della disciplina sulla concorrenza possa avere un impatto anche sulla tutela dei dati personali. A maggior ragione, dunque, un intervento sul piano tecnico contribuirebbe a garantire maggiormente il rispetto tanto dell'una quanto dell'altra disciplina. La soluzione più promettente è quella di favorire l'utilizzo integrato dei sistemi IoT e della tecnologia *blockchain*, anche, ma non solo, grazie agli *smart contract*. La parte conclusiva del capitolo è dunque dedicata all'esame di queste due tecnologie, nell'ottica del quadro giuridico attualmente vigente e delle potenziali incompatibilità fra queste ultime e la disciplina del GDPR.

Nel capitolo conclusivo s'intende dunque illustrare e dimostrare che integrando i sistemi IoT, la tecnologia *blockchain* e gli *smart contract*, è possibile non soltanto potenziare le prestazioni di ciascuna tecnologia individualmente considerata, ma anche ridurre i rischi legati alla tutela dei dati personali a cui sono esposti gli individui che le utilizzano. Muovendo dalle criticità precedentemente evidenziate, vengono dunque illustrate alcune possibili soluzioni tecniche che promettono di avere un impatto positivo in termini di maggior rispetto della disciplina del GDPR.

Si tratta peraltro di un'impostazione ispirata al principio di *privacy-by-design*, a cui il GDPR attribuisce grande importanza proprio perché coerente con l'idea di anticipare eventuali violazioni in ottica *"zero-risk"*.

Alla luce di quanto discusso in precedenza relativamente al fenomeno della "competizione sulla privacy" e alla tendenza a propendere per un approccio *ex ante*, è chiaro che queste soluzioni avrebbero un impatto positivo anche sulla tutela della concorrenza nel mercato interno. In primo luogo, se l'indirizzo inaugurato dall'Autorità tedesca con il caso Facebook trovasse definitiva applicazione a livello europeo, il rispetto della disciplina sulla tutela dei dati personali diverrebbe ancora più rilevante per le imprese di quanto non lo sia attualmente, dal momento che, in determinate circostanze, la sua violazione costituirebbe altresì un illecito concorrenziale. Intervenire a monte del problema darebbe loro maggiore sicurezza, riducendo il rischio di incorrere nell'irrogazione di sanzioni. Inoltre, garantendo *by-design* il rispetto del GDPR, si elimina il rischio di elusione di tale disciplina e la possibilità che questa si traduca un indebito vantaggio competitivo a favore di alcune imprese. Infine, integrare i sistemi IoT e la tecnologia *blockchain* favorirebbe e semplificherebbe l'esercizio del diritto alla portabilità dei dati, cruciale tanto per l'uno quanto per l'altro settore.

Nell'impossibilità proporre una soluzione unica e adattabile ad ogni contesto e nella piena consapevolezza che sarà necessario svolgere delle analisi concrete, condotte caso per caso e tenendo conto di tutte le circostanze rilevanti, si giunge a dimostrare che soltanto attraverso lo sviluppo parallelo di soluzioni tecniche e progresso normativo sarà possibile consentire una diffusione delle nuove tecnologie sostenibile non solo sotto il profilo giuridico, ma anche etico ed economico.

CAPITOLO I

I. Big Data: i rischi per la concorrenza e la tutela dei dati personali. Dal caso *Facebook (B6-22/16)* alle nuove prospettive di regolamentazione.

Questo capitolo si sofferma dapprima sul ruolo assunto dai dati nell'economia moderna, guardando al modo in cui i cosiddetti *"Big Data"* hanno cambiato i modelli di *business* adottati dalle imprese e messo a rischio la concorrenza. A partire da queste riflessioni, si passa dunque ad analizzare l'evoluzione del rapporto fra la disciplina sulla tutela dei dati personali e quella sulla concorrenza, alla luce del caso Facebook Germany (B6-22/16), che ha rappresentato un cambio di rotta rispetto alla tradizione giurisprudenziale dell'UE che aveva sempre tenuto ben distinto l'ambito di applicazione dell'una e dell'altra normativa. Il capitolo si chiude con una disamina del quadro normativo UE sulla tutela dei dati - ed in particolare dei dati personali – e delle nuove proposte della Commissione aventi ad oggetto la regolamentazione dei mercati digitali.

L'intersezione fra la disciplina del GDPR e il diritto alla concorrenza è la chiave di lettura che sarà seguita nel corso dell'intera indagine: la tesi che si vuole qui sostenere è che sfruttando la tecnologia *blockchain* e gli *smart contract* nel contesto dei sistemi *Internet of Things* sia possibile garantire un più alto livello di *compliance* di tali dispositivi rispetto alla disciplina UE sulla tutela dei dati personali e che, alla luce della stretta correlazione fra quest'ultima e il diritto alla concorrenza, ciò determini contestualmente degli effetti positivi per la salvaguardia del mercato interno.

1.1 Big Data: quanto valgono i dati nell'economia moderna

Negli ultimi anni è notevolmente cresciuta l'attenzione verso i cosiddetti *"Big Data"*, termine con il quale ci si riferisce alla grandissima mole di dati prodotti, raccolti e analizzati nell'industria moderna. Le tecnologie emergenti hanno facilitato la produzione, l'elaborazione, la raccolta, l'archiviazione e l'analisi dei dati. Se è pur vero, infatti, che la produzione di grandi quantità di dati è un fenomeno al quale si è iniziato ad assistere già con l'avvento dei primi computer, l'evoluzione tecnologica ha portato alla creazione di dispositivi in grado di raccogliere dati in modo continuo, sia attraverso l'interazione con l'ambiente circostante (ad esempio mediante sensori e videocamere), che con i soggetti che li utilizzano[6]. Si pensi, ad esempio, agli orologi in grado di rilevare il battito cardiaco o il numero di calorie consumate durante lo svolgimento di attività fisica, ai sistemi di riscaldamento in grado di misurare e

[6]Autorità Garante della Concorrenza e del Mercato (da qui in poi "AGCM"), *Big data, Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera* n. 217/17/CONS, accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf> (ultimo accesso 29 Aprile 2021).

adeguare automaticamente la temperatura o ai sistemi di tracciamento utilizzati comunemente dai telefonini.

Una delle innovazioni maggiormente rilevanti da questo punto di vista è senza dubbio l'*Internet of things*, locuzione con la quale – sebbene non esista une definizione generale - si fa riferimento a dispositivi connessi fra loro attraverso Internet, in grado non soltanto di raccogliere dati dall'ambiente circostante, ma anche di scambiarli reciprocamente, facendo crescere in misura esponenziale la quantità di dati disponibili. A ciò si aggiunga l'avvento di tecnologie come la *blockchain*, che consente il trasferimento e la condivisione dei dati in modo più semplice e sicuro, e della famiglia di tecnologie riconducibili alla nozione di AI, nella quale sono ricomprese le varie tipologie di algoritmi e sistemi utilizzati per la loro analisi ed elaborazione. I dati, infatti, non avrebbero alcun valore se non adeguatamente elaborati. L'elemento davvero rivoluzionario è rappresentato dunque dal raggiungimento di una notevole capacità e velocità di calcolo computazionale, nonché di conservazione dei dati (attraverso i *icloud*[7]) mai raggiunte prima.

Per descriverne adeguatamente le caratteristiche e le peculiarità, i Big Data sono tradizionalmente definiti mediante la regola delle cosiddette "3 V"[8]: volume, velocità e varietà, alle quali più recentemente sono state aggiunte altre "V", fra cui assumono particolare importanza la variabilità, il valore, la veridicità, la valenza e la visualizzazione. Con il termine Volume ci si riferisce alla grandezza dei dati, generalmente creati in settori quali la finanza o la sanità. La Velocità, invece, è valutata sia in relazione alla rapidità con cui tali dati vengono prodotti, che a quella con cui sono analizzati. La Varietà denota l'esistenza di diverse tipologie di Big Data, mentre la Variabilità si riferisce al modo in cui tali dati vengono raccolti. Il Valore è valutato in relazione all'importanza assunta sul mercato dai dati che vengono gestiti. La veridicità e la valenza sono in qualche misura ricollegate al valore, dal momento che attengono rispettivamente alla qualità dei dati e alla loro connessione con gli altri raccolti. La visualizzazione, invece, fa riferimento alla necessità di restituire i dati in una forma facilmente interpretabile, chiara e fruibile.

[7] Letteralmente "nuvola informatica", termine con cui ci si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso internet il c.c. consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale. Per le aziende di grosse dimensioni implica dunque un ingente abbattimento dei costi; non sono più necessari hardware potenti (costosi e soggetti a frequenti manutenzioni), ma basta una macchina in grado di far funzionare l'applicativo d'accesso alla "nuvola". Non mancano però le perplessità; da un lato i file sono accessibili solo tramite rete, dall'altro (nonostante le rassicurazioni dei fornitori) si teme per la sicurezza dei dati sensibili. Il c.c. può mettere a disposizione hardware in remoto (IaaS - *Infrastructure as a Service*), piattaforme *software* (PaaS - *Platform as a Service*) o software in remoto (SaaS - Software as a Service), Treccani, <https://www.treccani.it/enciclopedia/cloud-computing/>.

[8] AGCM, Autorità Garante delle Comunicazioni (da qui in poi AGCOM), Autorità Garante per la protezione dei dati personali (da qui in poi GPDP), *Indagine conoscitiva sui Big Data,* (2017), 8, accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf; Ali Dehghantanha e Kim-Kwang Raymond Choo, 2019 (ed. Cham: Springer International Publishing,) *Handbook of Big Data and IoT Security*, 6-7, accessibile da https://link.springer.com/book/10.1007%2F978-3-030-10543-3.

Non esiste una soglia dimensionale certa superata la quale è possibile far rientrare i dati trattati nella categoria dei Big Data, ma la classificazione si baserà sulle tecniche utilizzate per la loro analisi. Laddove non sia possibile il ricorso a sistemi di analisi tradizionale, si potrà parlare di Big Data.

Ai sensi dell'art. 4 del GDPR, s'intende per dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

La distinzione fra dati personali e non rileva dunque da un punto di vista giuridico poiché nel caso di trattamento di dati personali troverà applicazione la disciplina dettata dal GDPR, mentre in caso contrario si ricadrà entro l'ambito di applicazione del Regolamento (UE) 1807/2018, che disciplina la circolazione dei dati non personali all'interno dell'Unione Europea.

Il 15 dicembre 2020 la Commissione ha presentato inoltre due nuove proposte di Regolamento, il Digital Market Act[9] e il Digital Service Act[10], che hanno ad oggetto la regolamentazione dei mercati digitali e che, se approvate, influiranno sulla circolazione dei dati e soprattutto sul loro utilizzo a fini commerciali da parte delle grandi piattaforme digitali. L'avvento dei Big Data e lo sviluppo delle tecnologie a cui è fatto sopra riferimento, come IoT, *blockchain* e AI, mettono tuttavia in discussione la tradizionale distinzione fra le due categorie di dati[11]. Come si vedrà meglio nel prosieguo, infatti, la combinazione di *datasets* diversi e l'utilizzo di tecniche di analisi particolarmente sofisticate consentono di ottenere dati personali pur non disponendone inizialmente.

Sulla base della fonte dalla quale sono prodotti, possiamo distinguere almeno tre diverse categorie di dati[12]: i c.d. *open data*, cioè i dati - personali e no - raccolti dagli enti pubblici, i dati volontariamente forniti dagli utenti che accedono alle piattaforme digitali o utilizzano servizi IT e, infine, i dati generati dall'utilizzo di tali piattaforme e sistemi (es. cookies, ISP data).

L'importanza acquisita dai dati nell'economia moderna è tale che sempre più spesso questi vengono definiti come il "nuovo petrolio"[13]. L'utilizzo dei dati, infatti, gioca un ruolo fondamentale nei business

[9] Vedi nota 2.
[10] Vedi nota 3.
[11] AGCM, AGCOM, GPDP, (n. 8), 23.
[12] Björn Lundqvist, "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data", (Berlin, Heidelberg, Springer Berlin Heidelberg, 2018), 192, accessibile da https://doi.org/10.1007/978-3-662-57646-5_8,.
[13] European Parliament Think Thank, Is Data Protection the new oil? Competition Issues in the digital economy", (2020), accessibile da https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646117.

model delle aziende *BigTech*, le grandi piattaforme digitali che ad oggi dominano il mercato, come ad esempio le cosiddette "GAFAM" – acronimo riferito a Google, Amazon, Facebook, Apple e Microsoft.

Nel caso dei servizi offerti "gratuitamente" (es. alcune categorie *social network*), i dati forniti dagli utenti o generati automaticamente durante l'utilizzo delle piattaforme divengono di fatto la controprestazione dovuta per accedere al servizio. Il valore dei dati dipende da ciò che si può desumere analizzandoli: in altre parole, tramite "*letting the data speak*", (letteralmente "lasciar parlare i dati"), ossia traendone quante più informazioni possibili[14]. È mediante l'elaborazione di tali dati, infatti, che le imprese sono in grado di generare sponsorizzazioni mirate, i cui livelli di efficacia sono massimizzati proprio dalla "targetizzazione" dei destinatari. Anche nel caso di piattaforme come Amazon il controllo sui dati gioca un ruolo fondamentale, in quanto studiando e conoscendo le preferenze dei consumatori, la piattaforma è in grado di personalizzare l'esperienza del commercio online. Questi fattori hanno generato preoccupazioni sia per quanto riguarda il livello di concorrenza sul mercato, che in termini di tutela dei dati degli utenti, evidenziando la stretta correlazione fra le due discipline ed inducendo le istituzioni, soprattutto a livello europeo, ad intervenire regolamentando in modo innovativo questo settore. Si tratta, infatti, di problemi destinati a crescere nel futuro prossimo, di pari passo con lo sviluppo di nuove tecnologie che rendono sempre più semplice e veloce raccogliere, analizzare ed elaborare dati.

Per comprendere l'impatto che lo sviluppo delle piattaforme digitali ha avuto sulla quantità di dati generata oggigiorno, basta guardare alcuni dati riportati nell'indagine conoscitiva condotta congiuntamente dall'AGCM, dall'AGCOM e dal GPDP (risalente al 2017)[15]: ogni giorno nella sola Italia vengono vengono svolte 2,3 milioni di ricerche su Google, i tasti "mi piace" e "condividi" su Facebook vengono cliccati circa 3 milioni di volte, mentre su YouTube vengono effettuati circa 2,7 milioni di download, solo per citarne alcuni. Inoltre si stima che a livello globale entro il 2025 ci saranno più di 100 miliardi di sistemi IoT connessi, con un impatto sull'economia mondiale di circa $ 11 trilioni[16].

1.2 Il ruolo dei dati nei business model delle piattaforme digitali: l'evoluzione della giurisprudenza europea.

1.2.1 Le caratteristiche dei nuovi mercati

[14] Viktor Mayer-Schönberger e Yann Padova, "Regime Change? Enabling Big Data through Europe's New Data Protection Regulation", (2016), Science and Technology Law Review, 319, accessibile da https://doi.org/10.7916/stlr.v17i2.4007.
[15] AGCM, AGCOM, GPDP, (n. 8), 6.
[16] Karen Rose, Scott Eldridge, Lyman Chapin, "The Internet of Things: an overview. Understanding the issues and challenges of a more connected world", (2015), *The Internet Society*, 8, accessibile da https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.

L'utilizzo dei dati ha un'incidenza diversa sulla strategia economica delle imprese a seconda del tipo di mercato all'interno del quale queste operano.

Si distinguono, infatti, almeno tre categorie di mercati[17]. La prima è caratterizzata dal fatto che i dati rappresentano soltanto uno degli input impiegati dalle imprese nello svolgimento della propria attività. In questi settori l'avvento dei Big Data non ha rivoluzionato il modo di fare impresa, anche se influisce sui livelli di capacità produttiva. Per quello che qui interessa, in questi settori i dati non costituiscono un notevole vantaggio competitivo. La seconda categoria include i mercati in cui i dati vengono utilizzati per migliorare le offerte di beni e servizi rivolte ai clienti. I dati influenzano dunque le strategie di *marketing*, consentendo di adattare queste ultime alle preferenze e alle esigenze mostrate dai clienti (es. *search engine*). Per tale ragione si può dire che i dati giocano un ruolo importante nel determinare il vantaggio competitivo delle imprese. La terza categoria è quella che ha tratto maggior giovamento dal fenomeno del *datafication*, dal momento che vi rientrano quei settori in cui i dati hanno un'influenza diretta sulle caratteristiche dei beni e dei servizi offerti. Si potrebbe addirittura giungere a dire che senza l'utilizzo dei dati non sarebbe possibile neanche offrire determinati beni o servizi. In questi casi, infatti, i dati rappresentano per sé il prodotto o, comunque, si trovano in stretta correlazione con esso (es. *social network* o *applications* – da qui in poi *"app"* - *di dating*). Ci si trova solitamente di fronte a mercati in cui i servizi vengono offerti gratuitamente e i dati acquistano il valore di vera e propria controprestazione del servizio. Questa categoria include principalmente le attività svolte dalle piattaforme digitali, per le quali la possibilità di raccogliere, analizzare ed elaborare dati rappresenta un enorme ed importante vantaggio competitivo.

I mercati su cui operano le piattaforme sono mercati multilaterali, caratterizzati cioè dalla presenza di più gruppi che interagiscono fra loro su lati diversi del mercato[18]. Un esempio tipico è dato dai *social network*, in cui da un lato vi sono gli utenti iscritti per utilizzare il servizio social, mentre dall'altro operano i cosiddetti utenti *"business"*, che sfruttano la piattaforma per sponsorizzare i propri prodotti.

L'utilizzo dei dati assume un'importanza centrale nella strategia commerciale adottata, al punto da trasformarsi in vero e proprio vantaggio competitivo[19] e strumento per acquisire maggiore potere sul mercato. Al fine di comprendere in che modo le aziende sfruttano il valore economico dei dati e quali possono essere gli effetti distorsivi sulla concorrenza è necessario tenere conto di alcuni tratti peculiari di tali mercati[20]. In primo luogo, un ruolo fondamentale è svolto dal cosiddetto effetto di rete (*network*

[17] AGCM, AGCOM, GPDP, (n. 8), 70-71.
[18] Justus Haucap, 'Competition and Competition Policy in a Data-Driven Economy', (2019), vol. 54/no. 4 Inter Economics, 201, accessibile da https://link.springer.com/article/10.1007/s10272-019-0825-0.
[19] Lundqvist, (n. 12), 194-195.
[20] Autorità de la concurrence e Bundeskartellamt, *Report 'Competition law and data'*, (2016), 26-29, accessibile da https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=683860639BF2C0191A70260BE8486FDC.1_cid371?__blob=publicationFile&v=2; Haucap, (n. 18), 202-205.

effect)[21], sia diretto che indiretto. Nel caso delle piattaforme tale effetto rende indispensabile che queste siano sufficientemente ampie, affinché il loro utilizzo raggiunga dei livelli di efficienza soddisfacenti. Le concentrazioni[22] che hanno luogo sui mercati caratterizzati dagli effetti di rete non possono dunque essere valutate secondo gli stessi criteri adottati per i mercati tradizionali.

Questi mercati, infatti, hanno la naturale tendenza a convergere verso la creazione di monopoli, dal momento che la presenza di una sola piattaforma comporta la massimizzazione dell'effetto di rete rendendo il mercato sostenibile nel lungo periodo. Ad accrescere tale tendenza contribuiscono inoltre le economie di scala, perché le piattaforme sono caratterizzate da una struttura che impone costi fissi particolarmente elevati. Sono la (i) capacità limitata, (ii) la differenziazione dei prodotti e (iii) il *multi-homing*[23] a favorire, invece, la creazione di un sistema concorrenziale, bilanciando le naturali tendenze monopolistiche del mercato.

Bisogna infatti tenere a mente che la fonte principale di finanziamento delle piattaforme deriva dal cosiddetto "*targeting* comportamentale", ossia dal differenziare le offerte e i servizi proposti agli utenti sulla base delle preferenze e delle tendenze manifestate da questi ultimi[24]. L'efficacia di queste tecniche cresce in misura direttamente proporzionale alla mole di dati impiegata per "costruire" il profilo di ciascun utente e dunque alla sua accuratezza. Nei mercati *data-driven* (ossia "basati sui dati") è stata

[21] Per "effetto network diretto" s'intende l'utilità di un determinato bene o servizio cresce in misura proporzionale al numero di utenti che accedono al servizio stesso. L'esempio classico è rappresentato dai sistemi di telecomunicazione nei quali, tanto più cresce la comunità di utenti, quanto più questi godranno di un servizio migliore. Tale effetto, dunque, si produce in misura più evidente se il network di riferimento è particolarmente ampio. Gli "effetti indiretti", invece, riguardano i rapporti fra gli utenti che si trovano su lati opposti del mercato (es. imprenditori che utilizzano i servizi Facebook per sponsorizzare i propri prodotti e destinatari delle sponsorizzazioni). Implica, cioè, che l'aumento di utenti su uno dei due lati del mercato sia direttamente correlato all'aumento degli utenti sul lato opposto. (Autorité de la concurrence e Bundeskartellamt (n. 20), 27).

[22] Con il termine "concentrazioni" si fa riferimento in primo luogo alla fusione di due entità economiche totalmente distinte fra loro, che, estinguendosi, danno vita ad una entità terza e nuova. La nozione va estesa però anche a circostanze ulteriori, che includono ad esempio l'acquisizione di una società da parte di un'altra, nella misura in cui, in virtù di tale acquisizione, la prima goda di un potere di influenza decisiva sulla strategia commerciale e le scelte compiute dalla seconda. Nel novero delle concentrazioni va inclusa anche la creazione di *joint venture*, cioè di società nuove ma soggette al controllo totale delle società madri. Le ragioni che inducono le imprese a dar luogo a concentrazioni sono molteplici, partendo dall'incentivo alla creazione di economie di scala, sino a giungere all'acquisizione di maggiore potere di mercato. Altri benefici riconducibili alla fusione fra più imprese riguardano poi miglioramenti in termini di efficienza nel *management*, o anche contrastare le possibili uscite da un determinato settore. Tutti questi fenomeni possono però avere delle conseguenze rilevanti sul livello di concorrenza del mercato, ed è questa la ragione per cui la disciplina europea ha istituito dei meccanismi di controllo preventivi, attribuendo alla Commissione il potere di valutare, in casi specifici e secondo criteri determinati, i loro effetti orizzontali, verticali e conglomerali. Rispettivamente, si guarderà dunque agli effetti derivanti dalla fusione di imprese operanti all'interno dello stesso mercato, a quelli provocati dalla fusione di imprese operanti a livelli diversi della catena produttiva e, infine, alle distorsioni sulla concorrenza che la concentrazione potrebbe produrre su mercati diversi rispetto a quello in cui l'impresa è attiva, determinando l'esclusione dei concorrenti. Lo scopo di effettuare un controllo sulle concentrazioni non è collegato esclusivamente alla necessità di prevenire possibili abusi di posizione dominante, ma più in generale quello di garantire il mantenimento di livelli di concorrenza adeguati sul mercato, sempre nell'ottica di un maggiore benessere per i consumatori. La disciplina sulle concentrazioni presuppone un'analisi preventiva - e dunque in larga parte teorica - sugli effetti che la fusione fra due imprese può avere sulla concorrenza. L'autorità competente dovrà valutare non soltanto se l'impresa risultante dalla fusione avrà il potere di alzare i prezzi di determinati beni o servizi, ma anche se vi potrà essere un peggioramento in termini di output, qualità, varietà o innovazione. (Richard Whish e David Bailey "Competition Law", (Oxford University Press, 2018), 830-837).

[23] Con questo termine s'intende la possibilità per gli utenti di utilizzare contestualmente più piattaforme, senza che ciò comporti per loro un detrimento in termini sia economici che non.

[24] Autoritè de la concurrence e Bundeskartellamt, (n. 20), 8; Haucap, (n. 18), 207.

posta grande attenzione al fatto che in conseguenza della fusione fra due società, la risultante abbia la possibilità di accedere a nuovi *datasets* e dunque ad una quantità maggiore di dati[25]. Specialmente nel caso di fusioni fra grandi società e *newco*, limitare l'analisi a parametri puramente economici sarebbe infatti riduttivo e fuorviante, dato che queste ultime detengono quote di mercato poco significative e potrebbero non esservi sovrapposizioni orizzontali. Le autorità competenti dovranno dunque valutare gli effetti sulla concorrenza analizzando in che modo la fusione modifica la facoltà di accesso ai dati delle imprese e anche quale vantaggio acquisirebbe la risultante combinando dati diversi. Uno scenario diverso, ma comunque pericoloso in termini concorrenziali, verrebbe a delinearsi nel caso di una fusione fra imprese che godono già di un forte potere di mercato in mercati distinti, da cui i concorrenti potrebbero essere del tutto esclusi. Questo genere di valutazioni sono già confluite, come si vedrà a breve, nella *ratio decidendi* adottata dalla Commissione che, nella valutazione sulla compatibilità o meno delle operazioni con il marcato interno, ha dato rilevanza proprio al potere e al vantaggio competitivo che le piattaforme avrebbero potuto trarre dall'enorme mole di dati a loro disposizione e, soprattutto, sulle conseguenze per la concorrenza derivanti dall'utilizzo incrociato dei dati.

Il primo dei fattori summenzionati, (i) la capacità limitata, rileva sotto due diversi punti di vista. Da un lato, il numero eccessivo di sponsorizzazioni potrebbe produrre un effetto opposto a quello sperato, infastidendo e dunque allontanando l'attenzione dei consumatori. Dall'altro, l'accesso da parte di utenti diversi e la conseguente nascita di gruppi maggiormente eterogenei ha parimenti un impatto negativo sulla loro efficacia.

L'eterogeneità degli utenti e delle preferenze che questi manifestano è strettamente correlata anche al secondo degli elementi sopra indicati, ossia (ii) la differenziazione dei prodotti. Quanto più, infatti, differiscono fra loro le esigenze e le preferenze degli utenti, tanto più sarà più semplice per le piattaforme differenziare i propri prodotti, riducendo il rischio di concentrazioni.

(iii) Non si può infine trascurare l'effetto positivo sulla concorrenza generato dal *multi-homing*. Se, infatti, l'utilizzo di una piattaforma piuttosto che di un'altra non comporta costi aggiuntivi per l'utente, la contestuale sopravvivenza di più piattaforme è certamente più semplice. Meccanismo che non opera, ad esempio, nel caso dei *social network*, nei quali proprio in ragione dell'effetto *network* per i diversi gruppi di utenti non è vantaggioso scegliere di cambiare piattaforma.

Le piattaforme possono inoltre beneficiare dell'impiego dei dati in un contesto diverso rispetto a quello nel quale erano stati originariamente acquisiti, sfruttandoli cioè su diverse linee di *business*[26]. Alla luce

[25] Ibid., 16.

[26] Questo è ad esempio uno degli elementi più importanti nella strategia commerciale adottata da Amazon. Sfruttando la propria infrastruttura e i dati raccolti su livelli diversi, la società è stata in grado di favorire i propri prodotti a scapito di quelli dei concorrenti. L'infrastruttura di Amazon viene infatti utilizzata da diversi piccoli rivenditori per la diffusione dei propri prodotti. Mettendo a disposizione di questi ultimi la propria infrastruttura, la società è però al contempo in grado di raccogliere dati relativi alle preferenze dei consumatori, ai prodotti che vengono cercati e non trovati e così via. Tali informazioni consentono di

di ciò, è chiaro che il controllo dei dati costituisce per le imprese un vantaggio competitivo e una fonte di potere sul mercato, dal quale deriva il pericolo di innalzamento di barriere all'entrata e della creazione di monopoli[27]. Le piattaforme stanno dunque guidando la "*data-driven revolution*", forti del vantaggio competitivo di cui hanno goduto per essere state le prime a sfruttare economicamente i dati, e che stanno mantenendo grazie all'aggiornamento e al miglioramento continui dei sistemi di analisi[28].

1.2.2 I limiti dell'attuale disciplina sulla concorrenza

Di fronte a questo profondo cambiamento, la disciplina concorrenziale tradizionale si è rivelata inadeguata ad intercettare e frenare l'ascesa sul mercato delle nuove aziende *BigTech*, lasciando che queste acquisissero posizioni dominanti sul mercato.

a) Il mercato rilevante

La disciplina concorrenziale mira a tutelare le imprese, garantendo loro la possibilità di svolgere le proprie attività a condizioni eque rispetto agli altri concorrenti. L'applicabilità delle regole sostanziali dettate dal legislatore europeo dipende dalla definizione del cosiddetto mercato rilevante[29], che viene definito sotto due diversi profili: il mercato del prodotto[30] e il mercato geografico.

"personalizzare" l'esperienza del commercio online e di ridurre i rischi legati all'introduzione di nuovi prodotti sul mercato. Inoltre, i costi per entrare nel mercato delle piattaforme digitali sono molto alti e i vantaggi per le piattaforme già esistenti sono accresciuti dall'effetto *network*. In altre parole, la mole di dati di cui Amazon dispone si traduce per i concorrenti in una barriera di entrata nel mercato. Questo dimostra che la carenza dell'approccio tradizionale della disciplina concorrenziale almeno sotto due profili: la tendenziale qualificazione delle integrazioni verticali come non distorsive della concorrenza e la mancata considerazione dei dati quale elemento determinate nell'acquisizione di posizioni dominanti. L'errore più grande, però, è stato forse quello di continuare a guardare separatamente ai singoli mercati, limitando l'analisi al numero di utenti che ciascuna app o società fosse in grado di raggiungere, senza guardare al potere che potenzialmente potesse essere acquisito grazie all'utilizzo complessivo degli stessi. (Lina M. Khan 'Amazon's Antitrust Paradox', vol. 126 no. 3 *The Yale Law Journal*, (2017), 754-755, accessibile da https://www.yalelawjournal.org/note/amazons-antitrust-paradox).

[27] Autorité de la concurrence e Bundeskartellamt, (n. 20), 17.

[28] AGCM, AGCOM, GPDP, (n. 8), 20.

[29] Determinare il mercato rilevante è indispensabile per comprendere quali imprese siano effettivamente concorrenti dirette e se quindi la disciplina concorrenziale possa essere applicata o meno nei loro confronti. Il concetto di mercato rilevante del prodotto è stato elaborato in via giurisprudenziale dalla CGUE nel celebre caso "Continental Can" (Case 6-72 *Europemballage Corpn and Continental Can Inc v Commission* (JO)1972 L 7 25) in cui la corte ha annullato la decisione della Commissione secondo la quale l'impresa deteneva, insieme alla controllata SLW una posizione dominante su tre diversi mercati, evidenziando che la Commissione non avesse definito con sufficiente chiarezza perché si trattasse di tre mercati fra loro distinti. (Whish, Bailey, (n. 22), 26-29).

[30] Dopo incertezze iniziali sulla definizione di mercato del prodotto, in una Nota pubblicata dalla Commissione (Notice EC C372/5 [1997] accessibile da http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997Y1209(01):EN:HTML) sono stati individuati in modo più chiaro e sistematico gli elementi da tenere in considerazione. Posto che tale definizione ruota intorno al concetto di "sostituibilità" del prodotto, intesa nel senso che due o più prodotti possono dirsi appartenenti al medesimo mercato se possono facilmente essere scambiati l'uno con l'altro, era necessario individuare dei parametri oggettivi che consentissero di dare un'interpretazione uniforme e trasparente di mercato rilevante. La Nota individua tre elementi: (i) la sostituibilità dal lato della domanda, (ii) la sostituibilità dal lato dell'offerta, (iii) i concorrenti potenziali. Il primo fa riferimento al grado di sostituibilità di dei prodotti dal punto di vista dei consumatori ed è tradizionalmente considerato come il parametro più importante nella definizione di mercato rilevante. Il secondo, al quale viene invece normalmente attribuito carattere secondario, guarda al grado

Alcune delle caratteristiche tipiche dei mercati digitali influenzano notevolmente la definizione di mercato rilevante in questi settori.

Si è già avuto modo di parlare degli effetti *network*, delle economie di scala e degli *switiching costs*. Tutti questi fattori, contribuendo a rafforzare gli effetti *lock-in*[31] e scoraggiando il passaggio ad una piattaforma diversa da parte dei consumatori, determinano delle vere e proprie barriere all'entrata, influendo sulla definizione del mercato rilevante del prodotto.

L'elemento di maggior rilievo qui è però costituito dai potenziali concorrenti. Non a caso la Commissione ha generalmente fatto ricorso proprio a questo concetto per analizzare situazioni che, invece, nel modello americano venivano ricondotte al cosiddetto "mercato per l'innovazione"[32]. Con questa espressione la dottrina concorrenziale suole riferirsi a prodotti che pur non essendo ancora presenti sul mercato, potrebbero essere introdotti proprio grazie allo sviluppo e all'impiego di tecniche innovative. Quello che si suggerisce è che non bisogna guardare al mercato rilevante in senso statico, ma tenere conto anche dei potenziali sviluppi legati alla ricerca e all'innovazione. L'esistenza di concorrenti potenziali, cioè di soggetti che possono entrare a far parte del mercato, è stata assunta quale elemento di bilanciamento rispetto al potere di mercato detenuto dalle imprese già presenti.

Nei mercati digitali i potenziali concorrenti assumono un carattere molto più aggressivo rispetto a quanto avveniva in quelli tradizionali ed intervenire per tempo sul loro effettivo ingresso nel mercato rappresenta ad oggi una delle sfide maggiori del diritto antitrust[33]. Uno dei punti di forza delle piattaforme è dato proprio dal fatto che queste siano in grado di agire contestualmente su più mercati, sommando i vantaggi tratti da diverse linee di business. In questo senso si dice infatti che le *big tech* posseggono il "dono dell'ubiquità". Oltre alle risorse e alle infrastrutture su cui possono fare affidamento, è proprio la mole di dati di cui dispongono che ha consentito loro di cogliere le potenzialità

di sostituibilità dei prodotti dal punto di vista delle altre imprese. Ciò che rileva è dunque la facilità con la quale un'impresa può convertire la propria produzione a favore di un prodotto diverso. Bisognerà infine tenere conto del grado di facilità con cui altri concorrenti possono entrare sul mercato. Se il mercato è altamente dinamico e consente a nuove imprese di entrare facilmente a farne parte, il fatto che un'impresa detenga quote di mercato elevate avrà un'incidenza minore nel determinare il potere di mercato di cui effettivamente questa gode.

[31] Fenomeno che si verifica quando un agente, un insieme di agenti, o un intero settore sono intrappolati all'interno di una scelta o di un equilibrio economici dai quali è difficile uscire, anche se sono disponibili alternative potenzialmente più efficienti. Per i consumatori, si ha un fenomeno di *lock-in* quando i clienti sono legati a un venditore di beni e servizi e non possono utilizzare un altro fornitore senza incorrere in alcuni costi di transizione. Per es., molti prodotti elettronici, hardware o software, creano un effetto di *lock-in* a causa della compatibilità tra i diversi componenti fisici o tra i programmi software. (Treccani, "Dizionario di Economia e Finanza", (2012), accessibile da https://www.treccani.it/enciclopedia/lock-in_%28Dizionario-di-Economia-e-Finanza%29/#:~:text=lock%20in%20Fenomeno%20che%20si,disponibili%20alternative%20potenzialmente%20pi%C3%B9%20efficienti).

[32] Whish, Bailey, (n. 22), 38.

[33] AGCM, AGCOM, GPDP, (n. 8), 79; Mariateresa Maggiolino, "L'intelligenza artificiale e l'accesso ai dati: un ruolo per il codice del consumo e per il diritto antitrust" in Ruffolo, Ugo, Guido Alpa, Augusto Barbera, A. Barbera, G. Alpa, and U. Ruffolo *Intelligenza Artificiale: Il Diritto, i Diritti, l'Etica*, (Milano: Giuffrè Francis Lefebvre, 2020), 321.

di altri mercati, nonché di entrarvi e stabilizzarvisi assumendo e mantenendo una posizione dominante al loro interno.

Pur trattandosi di concorrenti soltanto potenziali, la loro presenza si traduce in un pericolo concreto e attuale per il mantenimento di un libero mercato concorrenziale. L'inadeguatezza dell'attuale disciplina, che ha consentito alle piattaforme digitali di acquisire un così vasto potere sul mercato, consiste proprio nel fatto che questa abbia continuato a guardare ai mercati singolarmente, senza considerare che proprio in virtù della mole di dati e delle tecniche di elaborazione e di analisi di cui queste società dispongono, l'accesso ai nuovi mercati è molto più semplice e redditizio di quanto non lo fosse in passato. Assicurare un'efficace applicazione della disciplina concorrenziale presuppone dunque un ripensamento della nozione di mercato rilevante, ampliata sino a ricomprendervi quei mercati su cui le piattaforme ancora di fatto non operano, ma che potrebbero facilmente essere aggrediti dalle stesse.

b) Il potere di mercato

Secondo fondamentale elemento da cui dipende la possibilità o meno di applicare la disciplina concorrenziale è il potere di mercato[34]. Un'impresa ha potere sul mercato quando è in grado di innalzare i prezzi per un determinato periodo di tempo o porre in essere altre pratiche assimilabili, ad esempio ridurre i livelli di produzione. Esistono tre diversi elementi che consentono di determinare l'effettivo potere di mercato detenuto da un'impresa: (i) la posizione di mercato di quest'ultima rispetto ai suoi concorrenti effettivi, (ii) la posizione rispetto ai concorrenti potenziali, (iii) il contro-bilanciamento di potere esercitato da clienti che godono di un forte potere contrattuale.

Con riferimento al primo degli elementi appena elencati, la disciplina tradizionale suole fare riferimento alle quote di mercato detenute da ciascun concorrente, assumendo queste ultime come indice rilevante della posizione di mercato detenuta. E' stato più volte ribadito che nel contesto dei mercati digitali è possibile individuare una nuova fonte del potere di mercato, rappresentata proprio dai dati che vengono ceduti alle imprese dai clienti o che le stesse sono in grado di raccogliere mentre questi ultimi usufruiscono dei servizi da loro offerti. Già nel contesto dei mercati tradizionali la Commissione aveva riconosciuto i possibili vantaggi competitivi derivanti da un'ampia disponibilità di dati[35]. Si trattava però di casi eccezionali, e i dati erano generalmente considerati alla stregua degli altri input utilizzati dalle imprese nella propria produzione. E' solo con l'avvento dei *big data* e la diffusione delle nuove tecnologie che il dibattito sulla centralità dei dati nell'economia si è fatto più acceso ed ha portato sia le

[34] Whish, Bailey, (n. 22), 42.
[35] Decisione della Commissione, *EDF/Dalkia en France* (Case COMP. M.7137), C(2014) 4438 final.

autorità nazionali che le istituzioni europee ad interrogarsi sulla possibilità di riconoscere un legame fra la disponibilità dei dati e il potere di mercato.

Il principale motivo per cui si negava che dalla disponibilità di dati discendesse un reale vantaggio competitivo è che questi sono considerati come beni non-rivali, cioè beni che – almeno in linea teorica – possono essere sfruttati contestualmente da più imprese, senza che ciò comporti una perdita di valore degli stessi[36]. Trattandosi di un bene di appartenenza non esclusiva, nessuna delle imprese operanti sul mercato si troverebbe in una situazione più favorevole rispetto alle altre, generando dei pericoli per la concorrenza.

Non si può però trascurare che nella prassi diversi fattori concorrono a limitare la disponibilità dei dati fra i concorrenti, minando alla base la tesi che ne esclude il valore competitivo[37]. Nei rapporti Business to Business (d'ora in poi "B2B"), infatti, la mancanza di adeguati incentivi economici e di fiducia fra gli operatori nell'utilizzo dei dati in modo rispettoso delle condizioni contrattuali, lo squilibrio nel potere di negoziazione fra le parti, il timore di interferenze da parte di soggetti terzi, nonché la poca trasparenza su chi possa utilizzare i dati e in che modo (ad esempio, nel caso di dati creati congiuntamente nell'ambito dei cosiddetti sistemi IoT), sono tutti fattori che contribuiscono a limitare fortemente il livello di condivisione dei dati. Inoltre alcune piattaforme hanno accesso a dati ulteriori, forniti loro da parti terze in virtù di specifici accordi o dal momento che queste forniscono, sponsorizzano o migliorano i propri beni e servizi operando sulle piattaforme stesse[38].

Più in generale, si può dire che l'effettivo vantaggio competitivo ottenuto dalle imprese in virtù dell'utilizzo dei dati dipende da molteplici fattori, fra cui – appunto – la possibilità o meno che questi siano accessibili da parte degli altri concorrenti o dal tipo di algoritmi utilizzati per elaborarli. Il valore dei dati dipende non tanto dai dati in sé, quanto dalle informazioni che è possibile ricavarne. L'impiego di algoritmi più complessi, in grado di generare risultati più precisi e variegati, consente dunque, a parità di tipologia e quantità di dati disponibili, di trarne un vantaggio maggiore.

A ciò va aggiunta un'altra considerazione, e cioè che ad oggi assistiamo ad una moltiplicazione delle fonti in grado di produrre dati, sia *online* che *offline*. Per descrivere questo fenomeno viene infatti spesso utilizzata l'espressione *"data is everywhere"*, a voler sottolineare che, proprio in ragione del fatto che i dati vengono prodotti non solo più facilmente, ma anche in quantità maggiore, i set di dati a disposizione delle imprese possa facilmente essere replicato dalle concorrenti[39]. Occorre fare però delle precisazioni[40]. In primo luogo, la raccolta di dati è possibile solo se le imprese sono dotate di

[36]Autorità de la concurrence e Bunderskartellamt, (n. 20), 36; Maggiolino, (n. 33), 316.
[37] Ibid, 38.
[38] Ibid, 34.
[39]AGCM, AGCOM, GPDP, (n. 8), 75.
[40]Autorità de la concurrence e Bunderskartellamt, (n. 20), 38-42.

infrastrutture adeguate, per le quali sono richiesti investimenti notevoli, nonché costi fissi elevati da sostenere abitualmente. Già questo primo elemento è sufficiente a far comprendere perché per le imprese più piccole è certamente più difficile raggiungere livelli di competitività soddisfacenti. In secondo luogo, se i dati vengono raccolti direttamente dagli utenti che usufruiscono di un determinato servizio, godranno di un effettivo vantaggio economico soltanto quelle imprese in grado di attrarre un numero sufficientemente alto di utenti, che sarà possibile raggiungere – e soprattutto mantenere - non solo grazie ad infrastrutture adeguate, ma anche grazie a notevoli investimenti in ricerca e innovazione.

Per non sostenere questi costi, le imprese potrebbero scegliere di acquistare da altre i dati di cui hanno bisogno. Anche questa alternativa non è però risolutiva nel definire dei corretti equilibri di mercato. In primis, la quantità di dati che un'impresa può acquistare da un'altra è certamente inferiore rispetto a quella a cui avrebbe accesso occupandosi della raccolta in modo diretto. Inoltre, il trasferimento dei dati fra imprese diverse potrebbe rivelarsi tecnicamente complesso o eccessivamente costoso a seconda del grado di interoperabilità fra i diversi sistemi. Potrebbero esservi poi dei limiti alla condivisione dei dati derivanti dagli accordi contrattuali o dalla regolamentazione, come accade ad esempio nel caso dei dati personali.

Questo porta anche ad una considerazione ulteriore, ossia al diverso valore attribuibile alle diverse tipologie di dati e al grado di sostituibilità di ciascuna. I dati personali, dai quali è possibile trarre maggiori informazioni sui consumatori anche ai fini della profilazione e della personalizzazione delle offerte, avranno chiaramente un valore economico maggiore rispetto ad altre categorie di dati, di cui deve tenersi conto nel determinare il potere di mercato.

Infine, le imprese potrebbero semplicemente scegliere di non condividere i dati di cui dispongono, proprio in ragione del fatto che questi costituiscono un vantaggio competitivo che sarebbe perso se anche gli altri concorrenti fossero in grado di sfruttarlo. A tutto ciò si aggiunga anche che il valore dei dati non dipende tanto dai dati considerati di per sé, quanto dal numero e dalla qualità delle informazioni che è possibile trarne[41]. Non può certo trascurarsi allora il ruolo giocato dagli algoritmi e dai sistemi di *data analysis* mediante i quali tali informazioni vengono concretamente estratte. In altre parole, il fatto che potenzialmente i dati grezzi siano a disposizione di tutti, non vuol dire che questi avranno per tutti lo stesso valore o si tradurranno nel medesimo guadagno in termini economici. Determinare se un bene sia o meno sostituibile ai fini concorrenziali, implica dunque determinare a monte il bisogno che quel bene è chiamato a soddisfare, ossia la funzione che esso svolge sul mercato[42]. In assenza di una valutazione che potremmo definire funzionale, nulla si potrà dire sul valore dei dati, né sul vantaggio competitivo ad essi riconducibile.

[41] Ibid, 42; AGCM, AGCOM, GPDP, (n. 8), 73.
[42] Maggiolino, (n. 33), 317.

c) Cartelli e pratiche concordate

L'avvento dei Big Data, ma soprattutto lo sviluppo di tecniche di analisi basate sull'utilizzo di algoritmi, pone dei problemi anche rispetto alla disciplina dettata dall'art. 101 del Trattato sul Funzionamento dell'Unione Europea (da qui in poi "TFUE") [43], che vieta gli accordi, le decisioni e le pratiche concordate restrittive della concorrenza.

Quanto ai primi, elemento determinante perché possa parlarsi di accordo è che vi sia stato l'incontro delle volontà delle parti, a prescindere dalla forma attraverso la quale questa venga manifestata [44]. Più complesso è determinare invece l'esistenza di una pratica concordata, poiché anche in questo caso è necessario, affinchè si configuri una violazione della disciplina concorrenziale, che il comportamento collusivo delle parti sia consapevole e voluto, ossia il frutto di contatti diretti o non fra di esse, sebbene in assenza di una prova tangibile[45]. L'accordo potrà dunque essere costituito da un contratto, dallo statuto di una società o, più semplicemente, dallo scambio di mail e altre comunicazioni fra le parti, mentre una pratica concordata potrà aversi anche in assenza di un contatto diretto. Occorre dimostrare che le scelte commerciali delle parti non siano soltanto il frutto del fisiologico adattamento alle condizioni di mercato, ma siano state comunemente concordate dalle imprese.

L'utilizzo di algoritmi per determinare le scelte commerciali da effettuare, potrebbe però porre dei problemi[46]. L'esempio a cui si fa maggiormente riferimento è quello degli algoritmi di prezzo, sulla base dei quali le imprese sono in grado di determinare il prezzo più vantaggioso a cui vendere i propri prodotti sul mercato. Gli accordi sui prezzi sono infatti espressamente indicati dal primo comma dell'articolo fra le attività sanzionate dalla disciplina europea. L'utilizzo diffuso di questi algoritmi, se da un lato comporterebbe maggiore trasparenza sul mercato, una migliore allocazione delle risorse e, quindi, un vantaggio collettivo in termini di competitività, dall'altro potrebbe produrre gli stessi effetti di un illegittimo scambio di informazioni, incompatibile con la portata della norma. Per quanto possa sembrare

[43] Versione consolidata del Trattato sul Funzionamento dell'Unione Europea, (2008), OJ C 115/13, art. 101(1) "Sono incompatibili con il mercato interno e vietati tutti gli accordi tra imprese, tutte le decisioni di associazioni di imprese e tutte le pratiche concordate che possano pregiudicare il commercio tra Stati membri e che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza all'interno del mercato interno ed in particolare quelli consistenti nel: a) fissare direttamente o indirettamente i prezzi d'acquisto o di vendita ovvero altre condizioni di transazione; b) limitare o controllare la produzione, gli sbocchi, lo sviluppo tecnico o gli investimenti; c) ripartire i mercati o le fonti di approvvigionamento; d) applicare, nei rapporti commerciali con gli altri contraenti, condizioni dissimili per prestazioni equivalenti, così da determinare per questi ultimi uno svantaggio nella concorrenza; e) subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi."

[44] Whish, Bailey, (n. 22), 102-103.

[45] Ibid, 115-117.

[46] Hennemann Moritz, "Artificial Intelligence and Competition Law" in Wischmeyer Thomas e Timo Rademacher *Regulating Artificial Intelligence*, (1st 2020. ed. Cham: Springer International Publishing, 2020), 373-375, accessibile da https://link.springer.com/chapter/10.1007%2F978-3-030-32361-5_16; Chauhan Sidharth, "Artificial Intelligence - a Competition Law Perspective", (2019), no. 3 *European Competition Law Review* 40, 139, accessibile da https://tinyurl.com/yf9qn2s5.

paradossale, l'eccessiva trasparenza sul mercato potrebbe passare dall'essere un vantaggio per i consumatori al rappresentare un pericolo.

Se il comportamento tenuto dalle imprese sul mercato non è più determinato da queste ultime sulla base di valutazioni autonome e indipendenti, quanto piuttosto condizionato da uno standard decisionale collettivo, non può più parlarsi di comportamenti paralleli compatibili con il normale andamento di mercato, ma di vere e proprie pratiche concordate. In alcuni casi si ritiene addirittura che possano configurarsi degli accordi fra le imprese. Questo potrebbe ad esempio avvenire grazie all'utilizzo di tecnologie *deep learning*[47], che permetterebbero alle imprese di calcolare il prezzo di vendita affinché tutte siano in grado di massimizzare i profitti senza incorrere nei rischi tipici della concorrenza. In entrambi casi fornire la prova di un comportamento anticoncorrenziale è certamente più difficile di quanto non lo fosse in passato.

La questione più dibattuta nell'ambito del discorso relativo ai rischi concorrenziali legati agli algoritmi verte sulla configurabilità di quel *"meeting of minds"*, ossia dell'incontro della volontà fra le parti, qualificato dalla Corte di Giustizia dell'UE (da qui in poi "CGUE") come elemento essenziale della collusione. Posto che le decisioni vengono assunte autonomamente dagli algoritmi, senza che sia necessario un reale scambio di informazioni fra i concorrenti, ci si chiede se effettivamente un incontro delle volontà possa dirsi raggiunto. Nell'affrontare tale questione parte della dottrina parte anzitutto dal presupposto che la configurabilità dell'elemento soggettivo non rileva ai fini dell'applicazione della disciplina concorrenziale europea e che quindi le scelte determinate degli algoritmi sono direttamente imputabili alle imprese che ne fanno utilizzo, senza che queste possano sottrarsi alla responsabilità che ne deriva[48]. Ritiene quindi che al tradizionale *"meeting of minds"* vada a sostituirsi quello che potrebbe essere definito *"meeting of algorithms"*, lasciando tuttavia aperto l'interrogativo sulla possibilità o meno che in tal caso si configuri una violazione dell'art. 101 TFUE.

d) Abuso di posizione dominante

L'art. 102 TFUE[49] mira a sanzionare l'abuso di posizione dominante da parte di un'impresa, se questo è pregiudizievole per il mercato interno o per una parte sostanziale dello stesso. La disciplina non

[47] Nell'Intelligenza Artificiale, classe di algoritmi di apprendimento automatico che utilizza livelli multipli per estrarre progressivamente caratteristiche di livello superiore dall'input grezzo. (Treccani, "Neologismi", (2019) accessibile da https://www.treccani.it/vocabolario/deep-learning_(Neologismi).

[48] Alberto Maria Gambino e Mariachiara Manzi, "L'intelligenza artificiale tra protezione del consumatore e tutela della concorrenza", in Ruffolo, Ugo, Guido Alpa, Augusto Barbera, A. Barbera, G. Alpa, and U. Ruffolo *Intelligenza Artificiale: Il Diritto, i Diritti, l'Etica,* (Milano: Giuffrè Francis Lefebvre, 2020), 332.

[49] Versione consolidata del Trattato sul Funzionamento dell'Unione Europea, (2008), OJ C 115/13, Art. 102(1): "È incompatibile con il mercato interno e vietato, nella misura in cui possa essere pregiudizievole al commercio tra Stati membri, lo sfruttamento abusivo da parte di una o più imprese di una posizione dominante sul mercato interno o su una parte sostanziale di questo. Tali pratiche abusive possono consistere in particolare: a) nell'imporre direttamente od indirettamente prezzi d'acquisto, di vendita

impedisce alle imprese di raggiungere una posizione dominante sul mercato, ma pone in capo a queste ultime delle responsabilità particolari[50]. La detenzione di una posizione dominante non si traduce in assoluta libertà per le imprese, ma anzi comporta l'insorgere di responsabilità ulteriori e più stringenti in capo a queste ultime. La disciplina europea mira ad assicurarsi che, anche in presenza di un'impresa dominante sul mercato, non abbiano luogo effetti distorsivi della concorrenza, che impediscano alle imprese concorrenti di esercitare liberamente e regolarmente le proprie attività sul mercato[51].

Il primo passo per l'applicazione dell'articolo consiste nel determinare se l'impresa abbia una posizione dominante. La definizione di tale nozione non è fornita dal legislatore, ma è frutto di elaborazione giurisprudenziale della CGUE, secondo la quale un'impresa può dirsi dominante quando è in grado di restare sul mercato operando in modo indipendente rispetto agli altri concorrenti, ai clienti e ai consumatori[52]. La Commissione[53] ha ulteriormente specificato che, perché possa dirsi dominante, l'impresa dovrà essere indipendente al punto che il comportamento tenuto dalle altre imprese, dai clienti e dai consumatori non influenzi in alcun modo le scelte assunte da quest'ultima.

I parametri adottati dalla disciplina tradizionale al fine di valutare la posizione di dominanza sono di natura strettamente economica. In primis si fa riferimento alle quote di mercato detenute in base all'ammontare del fatturato annuale e alla quantità di beni o servizi prodotti[54].

Nei nuovi mercati digitali, caratterizzati come detto dalla tendenziale gratuità dei prodotti o nei quali comunque il vantaggio competitivo delle aziende è strettamente legato ad un elemento di carattere non economico come il controllo sui dati, limitare l'analisi al fatturato o alle quote detenute non permette però di avere un quadro reale degli equilibri di mercato[55].

---

od altre condizioni di transazione non eque; b) nel limitare la produzione, gli sbocchi o lo sviluppo tecnico, a danno dei consumatori; c) nell'applicare nei rapporti commerciali con gli altri contraenti condizioni dissimili per prestazioni equivalenti, determinando così per questi ultimi uno svantaggio per la concorrenza; d) nel subordinare la conclusione di contratti all'accettazione da parte degli altri contraenti di prestazioni supplementari, che, per loro natura o secondo gli usi commerciali, non abbiano alcun nesso con l'oggetto dei contratti stessi.

[50] Whish, Bailey, (n. 22), 180-181.

[51] Per lungo tempo la disciplina europea sull'abuso di posizione dominante è stata criticata ed accusata di mirare a proteggere le imprese concorrenti piuttosto che la concorrenza di per sè. La critica proveniva soprattutto dalla dottrina americana, legata alla tradizione ordoliberale che concepiva la protezione dei consumatori quale fine ultimo della disciplina concorrenziale. La giurisprudenza della CGUE, ma anche le decisioni assunte dalla Commissione soprattutto negli ultimi anni, smentiscono tuttavia queste critiche, dimostrando che la disciplina europea mira alla protezione della concorrenza di per sé e, attraverso questa, al benessere dei consumatori (Whish, Bailey (n. 22), 201-203). Discutendo dello sviluppo di nuove tecnologie e della nascita dei nuovi mercati, è molto importante tenere a mente che gli sviluppi più recenti della disciplina concorrenziale vedono la tutela dei consumatori e il welfare come chiavi di lettura dell'art. 102 TFUE.

[52] Whish, Bailey, (n. 22), 187.

[53] Comunicazione della Commissione, *Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti* (2009) C45/7, para 10.

[54] Whish, Bailey, (n. 22), 189-190.

[55] Le riflessioni di Lina M. Khan, pur critiche verso la disciplina concorrenziale statunitense ed in particolare nei confronti l'approccio adottato dalla Scuola di Chicago, sono molto utili per comprendere come sia stato possibile per società come Amazon acquisire un tale potere sul mercato senza alcun intervento della disciplina concorrenziale. A parere dell'autrice l'errore è stato quello di focalizzarsi esclusivamente sull'interesse dei consumatori, senza guardare realmente alla struttura di mercato. Interesse di cui si è peraltro data un'interpretazione eccessivamente restrittiva, dal momento che gli esponenti della Scuola lo collegano

L'applicazione dell'articolo in esame presuppone anche la determinazione del mercato rilevante, alla luce degli elementi che sono stati sopra illustrati. Anche in questo caso valgono le considerazioni già svolte in relazione al contesto dei nuovi mercati digitali, in cui assume particolare rilevanza la valutazione dei cosiddetti concorrenti potenziali, dal momento che una serie di fattori tipici di queste nuove realtà rendono molto più semplice per le imprese estendersi su mercati diversi da quello in cui operano in via principale. In particolare la Commissione fa riferimento all'esistenza di barriere legali, vantaggi economici, costi ed effetti *network*, nonché alla condotta e al comportamento commerciale dell'impresa[56].

Fra i vantaggi economici rientra il controllo su quelle che vengono definite come *essential facilities*. La dottrina sulle *essential facilities* è stata introdotta dalla giurisprudenza europea con il caso *Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG* (Caso C-7/97, [1999]) e sancisce che, qualora un'impresa dominante sul mercato sia l'unica ad avere accesso ad un'infrastruttura ritenuta indispensabile per fornire un certo servizio, questa sia tenuta a consentirne l'utilizzo anche agli altri concorrenti[57]. Affinché trovi applicazione questo particolare obbligo è altresì necessario che l'infrastruttura in questione sia assolutamente non replicabile dalle altre imprese. Negarne l'accesso si tradurrebbe dunque in un'automatica esclusione delle stesse dal mercato, con un indebito vantaggio competitivo a favore della dominante. Questa pratica viene infatti annoverata fra quelle non tariffarie che possono dar luogo ad abusi di posizione. In questo caso un rifiuto a contrarre nel mercato a monte determinerebbe un danno concorrenziale a valle. L'elemento di non replicabilità è stato interpretato in senso lato, includendovi impedimenti materiali, legali ed economici[58].

Originariamente la dottrina delle *essential facilities* ha trovato applicazione in riferimento a strutture fisiche, quali porti, aeroporti o reti ferroviarie. L'avvento della quarta rivoluzione industriale e la nascita dell'economia *data-driven* ne hanno però suggerito una lettura ed un'interpretazione diverse, che assumono grande rilevanza nel discorso che si sta qui affrontando. Una tesi che sembra trovare sempre più sostegno è infatti quella di considerare i dati come *essential facilities*, imponendone alle imprese dominanti la condivisione con le concorrenti.

esclusivamente ad un vantaggio in termini di riduzione del prezzo, escludendo elementi come la qualità del prodotto, l'innovazione e la differenziazione. Il benessere dei consumatori è dunque valutato soltanto nel breve termine. In questo modo – sostiene l'autrice – si è persa l'occasione di cogliere per tempo gli effetti che la strategia economica di Jeff Bezos avrebbe prodotto nel medio e lungo termine. (Khan, (n. 26), 718-720).

[56] Whish, Bailey, (n. 22), 193-194.

[57] Ibid., 718.

[58] Per quanto concerne gli impedimenti materiali, si pensi ad esempio ad infrastrutture come porti e aeroporti. Potrebbero esservi ragioni ambientali o logistiche che impedirebbero la duplicazione delle suddette infrastrutture. Fra gli impedimenti legali, invece, possono annoverarsi i limiti derivanti dai diritti di proprietà intellettuale. Gli impedimenti di natura economica vanno intesi nel senso che dovrà valutarsi se il mercato sia in grado di sostenere o meno la presenza di un'altra infrastruttura. (Whish, Bailey, (n. 22), 719).

Per determinare se il rifiuto a condividere dati possa essere rilevante ai fini dell'applicabilità dell'art. 102 TFUE andrà anzitutto chiarita la finalità per cui è richiesto l'accesso a questi ultimi[59]. In generale, i dati vengono richiesti se ritenuti necessari per a) offrire un bene od un servizio al consumatore, nel medesimo mercato in cui opera l'impresa dominante, b) competere su un mercatato contiguo, c) competere su un *aftermarket* (mercato a valle). Per verificarne l'indispensabilità ai sensi di quanto previsto dalla disciplina comunitaria avranno poi rilevanza la natura dei dati (ed in particolare se si tratti o meno di dati personali), le modalità con cui questi sono stati raccolti (se volontariamente forniti dal consumatore o ricavati dall'impresa mediante *data analysis*), il loro grado di aggregazione. Non sempre, né automaticamente, i dati saranno dunque qualificabili come *essential facilities*, nonostante la loro rilevanza economica e lo stretto legame che sussiste fra il loro utilizzo e il mantenimento di un equilibrio sul mercato. Dovrà comunque essere accertato che il rifiuto di condividere i dati comporti effettivamente l'esclusione del concorrente dal mercato o che si traduca in un danno diretto per il consumatore.

La giurisprudenza tende ad applicare cautamente questa dottrina al contesto dei mercati digitali, sia perché riconosce che l'utilizzo dei dati nell'economia si traduce anche in un vantaggio per i consumatori in termini tanto di innovazione quanto di migliore qualità dei prodotti, sia perché bisogna considerare che vi sono casi in cui i dati sono effettivamente a disposizione di tutti i concorrenti. Inoltre, come si è già osservato, il vantaggio competitivo deriva in larga parte dalle tipologie di algoritmi utilizzati e dal grado di sviluppo degli stessi che dai dati trattati. In ogni caso applicare la dottrina delle *essential facilities* ai dati potrebbe far sorgere dei problemi di compatibilità con la disciplina del GDPR, poiché nel caso di dati personali la loro condivisione con soggetti terzi presuppone il previo consenso da parte dell'interessato o comunque la possibilità di invocare una delle altre basi giuridiche previste dal GDPR.

Fra i sintomi dell'esistenza di una posizione dominante sono poi annoverabili tutti quei fenomeni in grado di favorire i cosiddetti effetti *lock-in*, escludendo gli altri concorrenti dal mercato, o rendendone comunque particolarmente difficile l'accesso. Bisogna allora chiamare ancora una volta in causa gli effetti *network* e gli *switching costs* che divengono delle vere e proprie barriere all'entrata per i concorrenti. Si tratta di concetti già utilizzati dalla Commissione in passato, come nella decisione su *Microsoft Corp. v Commission* (Case T-2021/04) o nel caso *Google and Alphabet v Commission* (Case T-612/17), la cui rilevanza cresce in maniera proporzionale allo sviluppo e alla diffusione delle nuove tecnologie.

Rilevano infine la condotta e l'attività economica portate avanti da un'impresa, considerati anch'essi indici significativi di una possibile posizione dominante. Rientrano ad esempio in questa definizione sia l'imposizione di prezzi discriminatori o di condizioni particolarmente svantaggiose per i concorrenti. Su

[59] AGCM, AGCOM, GPDP, (n. 8), 109-110; Autoritè de la concurrence e Bunderskartellamt, (n. 20), 18.

questo punto può dunque nuovamente tirarsi in ballo il rapporto fra concorrenza e tutela dei dati personali.

Non si è mancato di mettere in luce che nei mercati *zero-price* la tutela dei dati personali è uno degli elementi che determina la qualità di un prodotto. Può ben dirsi che se un'impresa è libera di ridurre i livelli di modificare le condizioni dettate dalle *privacy policy* in senso peggiorativo per i consumatori, cioè riducendo gli standard di protezione dei dati personali, senza che ciò comporti per essa una perdita, tale condotta manifesti l'esistenza di un notevole potere di mercato in capo alla stessa[60]. In molti casi infatti i consumatori, sebbene consapevoli dei rischi in cui incorrono i loro dati personali, non godono di una reale possibilità di scelta e ciò è senz'altro sintomatico dell'esistenza di un notevole potere di mercato in capo all'impresa dominante, a maggior ragione in quei mercati in cui i prodotti sono offerti gratuitamente e il trattamento dei dati personali è direttamente collegato alla principale fonte di remunerazione delle imprese. Il danno sofferto dai consumatori non si limita necessariamente ad un danno di natura economica, ma include anche peggioramenti in termini di varietà, qualità e innovazione dei prodotti[61].

1.2.3 La tutela dei dati personali come elemento rilevante per la concorrenza: l'evoluzione giurisprudenziale.

Tanto la giurisprudenza europea, quanto le corti degli Stati Membri a livello nazionale, hanno escluso per lungo tempo la possibilità di integrare la disciplina concorrenziale con altre branche del diritto, ferme nella convinzione che le regole sulla concorrenza mantenessero un ambito di applicazione autonomo e distinto rispetto agli altri settori[62], basandosi sul presupposto che ciascuna disciplina nasce dall'esigenza di tutelare posizioni diverse. Con il passare del tempo, è emersa però l'esigenza di fare riferimento a parametri nuovi, iniziando a riconoscersi una tendenziale convergenza fra la disciplina concorrenziale e altre discipline quali quella sulla protezione dei dati personali, sulla tutela dei consumatori e sulla proprietà intellettuale (d'ora in poi "IP"), proprio in virtù del ruolo giocato dai dati nel nuovo business model italiano delle società[63].

Questo è quanto emerge, ad esempio, dal caso *Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL v Asociación de Usuarios de Servicios Bancarios* (Case C-238/05), in cui la CGUE ha affermato espressamente che qualunque questione attinente alla protezione dei dati personali fosse del

[60] Samson Y Esayas, "Competition in (Data) Privacy: 'zero'-Price Markets, Market Power, and the Role of Competition Law", (2018), Vol. 8 No. 3 International Data Privacy Law, 181-182, accessibile da https://academic.oup.com/idpl/article/8/3/181/5198968; José Tomás Llanos, "A Close Look on Privacy Protection as a Non-Price Parameter of Competition" (2019), vol. 15/no. 2-3 European Competition Journal, 233, accessibile da https://www.tandfonline.com/doi/full/10.1080/17441056.2019.1644577.
[61] Llanos, (n. 60), 234.
[62] Autoritè de la concurrence e Bundeskartellamt, (n. 20), 22-23.
[63] AGCM, AGCOM, GPDP, (n. 8), 100-102.

tutto irrilevante per la disciplina concorrenziale e andasse valutata e risolta soltanto alla stregua della disciplina di settore adottata dal legislatore europeo.

Orientamento confermato anche dalla successiva decisione della Commissione sulla fusione fra Google e DoubleClick[64] risalente al 2008. Nel caso di specie la Commissione era stata chiamata a valutare se l'acquisizione di DoubleClick da parte di Google potesse inficiare o meno la libera concorrenza nel mercato interno dell'UE. Google svolgeva contestualmente sia attività di intermediazione nell'ambito dei servizi di sponsorizzazione, sia attività di semplice sponsorizzazione online, mentre DoubleClick forniva esclusivamente un servizio di sponsorizzazione, che gli utenti avrebbero potuto utilizzare congiuntamente anche ad altri servizi di intermediazione oltre a quello offerto da Google.

L'analisi svolta dalla Commissione si è basata sia sugli effetti orizzontali dell'acquisizione, sia su quelli verticali. Nel valutare le possibili conseguenze distorsive della concorrenza, la Commissione ha sì tenuto conto degli effetti derivanti dalla combinazione dei *datasets* detenuti dalle due società, ma senza prendere in considerazione gli eventuali impatti in termini di tutela dei dati. La decisione, elaborata dunque sulla base di criteri strettamente economici, è stata nel senso di ritenere l'acquisizione compatibile con le regole stabilite per il mercato interno dell'UE, in quanto, a parere della Commissione, la società risultante non avrebbe ottenuto una posizione ed un potere di mercato tali da poter escludere i propri concorrenti e dunque impedire la libera concorrenza. In particolare, la Commissione ha affermato che la società non sarebbe stata in grado di imporre ai propri clienti condizioni contrattuali che consentissero l'utilizzo dei dati in modo incrociato.

Intravedendo però i possibili rischi in termini di tutela dei dati personali, nella stessa decisione la Commissione ha ribadito che l'acquisizione non facesse comunque venir meno gli obblighi derivanti dalla disciplina sulla tutela dei dati personali, sottolineando la propria competenza a vigilare sul rispetto della stessa. Seppure consapevole dei possibili rischi in termini di protezione dei dati personali, la Commissione ha dunque ancora una volta tenuto ben distinta l'applicazione delle due discipline.

Anche nel 2014, chiamata a pronunciarsi sulla fusione fra Facebook e Whatsapp[65] la Commissione ha confermato la separazione fra l'ambito di applicazione della disciplina concorrenziale e quella relativa alla protezione dei dati personali, pur compiendo un passo avanti rispetto alle decisioni precedenti[66].

---

[64]Commissione, Decision declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement, COMP/M.4621 *Google/DoubleClick* (2008), accessibile da https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf; Giuseppe Colangelo, Mariateresa Maggiolino, "Data Protection in Attention Markets: Protecting Privacy through Competition?", (2017), vol. 8 no. 6 *Journal of European Competition Law & Practice,* 365, accessibile da https://academic.oup.com/jeclap/article/8/6/363/3812670.

[65] Commissione, Decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004 (Caso COMP/M 7217 - *Facebook/Whatsapp*, (2014), accessibile da https://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.

[66]Colangelo, Maggiolino, (n. 64), 365-366; Marija Stojanovic, "Can Competition Law Protect Consumers in Cases of a Dominant Company Breach of Data Protection Rules?", (2020), no. 2-3 *European Competition Journal*, 540, accessibile da https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1824464.

Viene infatti affermato per la prima volta che gli standard di tutela dei dati personali rappresentano uno degli elementi che concorrono a determinare la qualità del servizio offerto. Anche in questo caso la Commissione ha valutato la compatibilità dell'acquisizione rispetto alle regole del mercato interno, interrogandosi sulle possibili conseguenti restrizioni o limitazioni della concorrenza e sull'eventuale pregiudizio sofferto dagli altri concorrenti sul mercato. La Commissione ha infine fornito un parere positivo sulla base dei seguenti elementi: (i) Facebook e WhatsApp non sono concorrenti diretti, circostanza confermata dal fatto che entrambe le applicazioni sono spesso utilizzate contestualmente dagli utenti, (ii) i consumatori possono facilmente passare all'utilizzo di applicazioni diverse, senza che ciò comporti per loro costi o oneri aggiuntivi. A sostegno di questa tesi, la Commissione ha sottolineato in particolare che le *app* sono fruibili gratuitamente e le informazioni su di esse facilmente rinvenibili e accessibili ai consumatori, (iii) con riferimento al mercato dei *social network*, la Commissione ha evidenziato che la presenza di fattori quali, ad esempio, la possibilità per gli utenti di utilizzare contestualmente più *app* di comunicazione evitando la creazione del cosiddetto "effetto *lock-in*", siano sufficienti a mitigare gli esistenti effetti di rete. Parimenti, la Commissione ha escluso che gli effetti di rete potessero essere amplificati dalla fusione delle due società, poiché ciò sarebbe possibile solo nel caso di integrazione dei servizi offerti dalle due piattaforme, ipotesi considerata di difficile attuazione tecnica e comunque esclusa da Facebook, (iv) quanto al mercato dei servizi di sponsorizzazioni online, la Commissione ha stabilito che anche in seguito alla fusione, Facebook non sarebbe stata in grado di migliorare i propri servizi utilizzando i dati raccolti tramite l'utilizzo di WhatsApp da parte degli utenti. E' stato escluso che WhatsApp possa introdurre altre sponsorizzazioni personalizzate, in quanto ciò avrebbe presupposto una previa modifica delle *privacy policy* sottoscritte dagli utenti, giudicata dalla Commissione non conveniente per la società. Agli occhi della Commissione, a tale cambiamento e al conseguente deterioramento del livello di tutela dei dati personali, gli utenti potrebbero rispondere scegliendo di utilizzare un altro servizio.

Le conclusioni qui esposte si sono rivelate errate sotto diversi profili, specie con riguardo all'impossibilità di integrazione fra le due piattaforme ed ai possibili vantaggi competitivi che Facebook avrebbe potuto trarne. Due anni dopo l'assunzione della decisione in esame, Facebook ha infatti modificato le condizioni contrattuali sottoscritte dagli utenti, al fine di consentire l'utilizzo incrociato dei dati raccolti attraverso WhatsApp e di quelli ceduti direttamente a Facebook. Nel 2017 la Commissione si è dunque pronunciata nuovamente[67], sanzionando Facebook al pagamento di un'ammenda per aver fornito informazioni inesatte o fuorvianti sull'effettivo utilizzo dei dati in seguito alla fusione.

[67] Commissione, Decision imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for supply by an undertaking of incorrect or misleading information, Caso M.8228 - *Facebook/WhatsApp* (2017), accessibile da https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf.

Dall'analisi dell'originaria decisione assunta dalla Commissione, emerge che la valutazione svolta da quest'ultima fosse errata almeno sotto due profili[68]. Anzitutto, la Commissione ha erroneamente ritenuto che il comportamento degli utenti potesse concretamente influenzare le scelte della società, arginando i rischi in termini concorrenziali. Il fatto che, nonostante il cambiamento delle condizioni contrattuali, WhatsApp non abbia subito una significativa perdita nel numero di utenti iscritti al servizio, dimostra invece che il potere esercitato da questi ultimi sulle scelte concorrenziali adottate dalla società è praticamente nullo. Fra le ragioni di questo fenomeno vi sono certamente lo squilibrio di potere e l'asimmetria informativa che caratterizza il rapporto fra la piattaforma e l'utente. Nel caso di specie, il cambiamento delle condizioni contrattuali non era stato adeguatamente segnalato e comunicato in maniera tale che non aderirvi fosse complesso e non immediato per gli utenti[69]. Il secondo elemento che ha indotto in errore la Commissione è l'aver valutato come non vantaggiosa o addirittura sconveniente un'eventuale modifica delle condizioni dettate dalla *privacy policy* dopo la fusione[70]. Anche nell'ipotesi in cui il cambiamento delle suddette condizioni avesse comportato una perdita nel numero di utenti iscritti al servizio, infatti, non era comunque escluso che il margine di guadagno derivante dalla possibilità di utilizzare in modo combinato i dati delle due piattaforme, personalizzando i servizi offerti e massimizzando la redditività delle sponsorizzazioni, fosse superiore alla perdita subita.

Un altro caso che ha segnato l'evoluzione dell'orientamento della Commissione è quello della fusione fra Microsoft e LinkedIn[71]. Anche in questo caso la Commissione ha espresso il proprio parere positivo sull'acquisizione del *social network* da parte di Microsoft, pur manifestando delle preoccupazioni in merito alle possibili conseguenze negative in termini di capacità di scelta dei consumatori sulle opzioni relative alla tutela dei propri dati personali[72]. Nel caso di specie, infatti, la Commissione si è soffermata sugli effetti che seguirebbero all'eventuale pre-installazione del *social network* sui sistemi offerti da Microsoft e dall'integrazione dei servizi offerti dalle due piattaforme. Per la prima volta il livello di controllo esercitato dagli utenti sui propri dati personali viene tenuto in considerazione dalla Commissione al fine di determinare il potere di mercato e i possibili profili di abusi concorrenziali. Nella decisione si legge infatti che l'integrazione fra i servizi potrebbe portare all'esclusione dal mercato di altri concorrenti, nonostante questi offrano ai propri utenti condizioni migliori in termini di tutela dei dati personali. In questo modo la Commissione riconosce la tutela dei dati e il controllo esercitato su di essi da parte degli utenti come parametri non economici a cui fare riferimento nell'analizzare i profili

[68] Esayas, (n. 60), 195-196.
[69] In primo luogo, il messaggio mostrato agli utenti non faceva alcuna menzione della possibilità per Facebook di utilizzare i dati raccolti attraverso WhatsApp. Inoltre, la piattaforma aveva disposto la pre-selezione dell'accettazione dei nuovi termini della privacy policy, richiedendo all'utente di utilizzare altri link per accedere alle informazioni ulteriori e disattivare l'opzione.
[70] Esayas, (n. 60), 196.
[71] Commission, Decision pursuant to Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation No 139/2004 and Article 57 of the Agreement on the EEA, (Case M.8124 - *Microsoft / LinkedIn* (2016), accessibile da https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf.
[72] Esayas, (n. 60), 199.

concorrenziali. Sebbene per la prima volta rilevi in maniera considerevole l'importanza attribuita dalla Commissione alla tutela dei dati personali e al rispetto della disciplina dettata dal GDPR, al punto che ne viene fatta espressa menzione anche come limite all'utilizzo che la società risultante potrà fare dei dati acquisitivi, la decisione in esame non si discosta comunque dalla giurisprudenza precedente, escludendo una vera integrazione fra la disciplina sulla tutela dei dati personali e quella concorrenziale [73].

Dall'analisi dei seguenti casi emerge una crescente consapevolezza, basata anche sulle tendenze manifestate dalle corti e dalle autorità competenti a livello nazionale, che le questioni concernenti la protezione dei dati personali non possano essere a priori escluse dalle indagini condotte nell'ambito del diritto della concorrenza, specialmente in quei casi in cui la raccolta dei dati da parte di un soggetto che opera in posizione dominante ha un ruolo strategico nel suo *business plan*, ed è dunque direttamente correlato all'equilibrio del mercato[74].

Dal momento che fra i dati vi sono anche e soprattutto dati personali, maggiore sarà l'attenzione posta dai consumatori alle modalità di trattamento dei loro dati, maggiore sarà l'incidenza in termini competitivi delle norme che le imprese sono chiamate ad applicare nell'effettuare tale trattamento. Si è giunti a parlare addirittura di "competizione sulla privacy" alludendo proprio all'influenza che tale disciplina esercita sulla scelta dei consumatori di acquistare o meno determinati beni e/o usufruire di specifici servizi[75].

Nel valutare quanto i livelli di protezione dei dati personali offerti dalle società influenzino concretamente le scelte dei consumatori, occorre tenere però conto del cosiddetto "paradosso sulla privacy"[76]. Con questa espressione ci si riferisce al fenomeno per cui, nonostante i consumatori siano consapevoli dei rischi legati alla protezione dei propri dati personali e manifestino preoccupazioni a riguardo, queste non abbiano alcun riflesso sul comportamento e le scelte da loro concretamente adottate, continuando a preferire servizi che offrono standard di protezione inferiori rispetto ad altri.

---

[73] Stojanovic, (n. 66), 541.

[74] Autorità de la concurrence e Bundeskartellamt, (n. 20), 11. Anche negli Stati Uniti si registra un cambio di rotta rilevante rispetto al passato, come dimostrato dalla la recente azione intrapresa della Federal Trade Commission (FTC), decisa a chiedere la dismissione di WhatsApp da parte di Facebook. Non a caso il Financial Times lo ha definito il primo vero caso "post-liberale" sulla concorrenza, che si differenzia da tutte le azioni anti-monopolistiche intraprese in precedenza proprio perché pone l'accento sulla limitazione del controllo sui dati. Soprattutto dopo l'elezione di Biden, ci si aspetta che il diritto antitrust statunitense si prepari a vivere una stagione di rinnovamento. (Rana Foroohar, "The FTC strikes back against Facebook", *The Financial Times*, 14 dicembre 2020, 21).

[75] Francisco Costa-Cabral e Orla Lynskey, "Family Ties: The Intersection between Data Protection and Competition in EU Law", (2017), *54*, no. 1 *Common Market Law Review*, 8, accessibile da http://eprints.lse.ac.uk/id/eprint/68470. Sotto questo profilo è importante sottolineare che la differenza sostanziale che si registra fra la realtà europea e quella statunitense potrebbe avere delle conseguenze rilevanti anche sul successo della nuova regolamentazione che l'UE sta preparando. Diversi sondaggi, infatti, evidenziano maggiore consapevolezza e attenzione sui rischi legati alla tutela dei dati personali da parte dei cittadini europei, rispetto a quelli americani. ("Europe's beef with GAFA – big tech faces competition and privacy concerns in Brussels", (2019), The Economist, accessibile da https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels).

[76] Stojanovic, (n. 66), 535.

Consapevole che le esigenze poste dall'economia moderna non possono più essere ignorate e cogliendo anche la maggiore sensibilità dimostrata in questo senso da alcune corti nazionali come ad esempio quella tedesca, l'European Data Protection Supervisor (qui di seguito "EDPS")[77] ha incoraggiato una maggiore cooperazione fra le autorità competenti in settori diversi, quali la concorrenza, la tutela dei dati personali e la tutela dei consumatori, evidenziando che la disciplina sulla tutela dei dati personali potrebbe essere assunta quale parametro di riferimento in casi concernenti le fusioni fra società, per determinare il rischio di concentrazioni ad esse collegato, o quale indice rilevante nelle ipotesi di abuso di posizione dominante.

La disciplina sulla tutela dei dati personali svolge contestualmente il ruolo di doppio limite di quella sulla concorrenza: da un lato ne influenza la logica interna, dall'altro ne condiziona l'applicazione, in virtù del suo carattere di diritto fondamentale[78]. A favore di questo orientamento gioca anche il fatto che entrambe le discipline, sebbene mantengano ambiti di applicazione distinti, abbiano obiettivi comuni: il rafforzamento del mercato interno e la protezione degli individui. Mentre l'una persegue tali obiettivi incidendo sulle scelte individuali riguardanti l'utilizzo dei dati personali, l'altra lo fa regolando il comportamento sul mercato dei vari concorrenti.

La convergenza fra la disciplina sulla concorrenza e quella relativa alla tutela dei dati personali sembrerà forse meno sorprendente se si tiene conto del fatto che a livello nazionale le Autorità competenti hanno già accolto la possibilità di ammettere possibili integrazioni fra discipline diverse, ad esempio fra la disciplina concorrenziale e quella sulla tutela dei consumatori.

Basti in tal senso l'esempio fornito dalla pronuncia dell'AGCM contro Facebook sulle regole di raccolta dei dati acquisiti tramite soggetti terzi[79] che, a parere dell'Autorità, violano la disciplina italiana sulla tutela dei consumatori. Nella relazione, l'AGCM svolge delle considerazioni sul *business model* della società, evidenziando la centralità dell'utilizzo dei dati. La società ha tentato di difendersi appellandosi all'impossibilità di utilizzare norme concernenti la tutela dei dati personali al fine di configurare un danno ai consumatori, mentre l'AGCM ha sostenuto la propria tesi evidenziando che definire gratuito l'accesso al servizio sia fuorviante e induca in errore i consumatori, dal momento che questi interpretano il termine "corrispettivo" in senso tradizionale, identificandolo cioè con l'obbligazione ad una prestazione pecuniaria. I servizi offerti da Facebook, invece, vengono "pagati" mediante la cessione di

[77] EDPS, *Privacy and competitiveness in the age of big data*, (Preliminary opinion, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

[78] Costa-Cabral, Lynskey. (n. 75), 8-10.

[79] AGCM, *Facebook-Condivisione Dati Con Terzi* (Provvedimento n. 27432, 2018), accessibile da http://www.agcm.it/dotcmsCustom/tc/2023/12/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/5A1EFA963A109B64C125835F00542FE2/%24File/p27432.pdf.

dati personali. È chiaro, dunque, che la disciplina concernente la tutela di tali dati possa (anzi, debba) essere assunta quale parametro di riferimento nel valutare la sussistenza di un danno ai consumatori.

L'AGCM ha peraltro di recente sanzionato Facebook per non avere ottemperato agli ordini impartiti con la suddetta decisione[80]. La società ha quindi presentato ricorso al TAR Lazio contro la suddetta delibera[81] e quest'ultimo, con le sentenze 260/2020 e 261/2020, ha accolto l'istanza cautelare e parzialmente il ricorso, dichiarando l'annullamento soltanto con riferimento ad una delle due pratiche contestate[82], ed in particolare quella relativa alla trasmissione e l'utilizzo dei dati personali degli utenti, lasciando a questi ultimi soltanto la possibilità di esercitare l'opzione *opt-out*. Sia l'AGCM che Facebook si sono allora rivolti al Consiglio di Stato, presentando ricorso per chiedere rispettivamente l'annullamento del provvedimento relativo alla pratica b) e della conferma della delibera 27437/2018 sulla pratica a). Con la sentenza n. 2360/2021, il Consiglio di Stato[83] ha respinto entrambi i ricorsi, affrontando preliminarmente la questione concernente la non commerciabilità dei dati personali, su cui si basava la difesa di Facebook. La società, infatti, appellandosi alla natura di diritto fondamentale dei dati personali riteneva non applicabile ad essi la disciplina sul consumo. Nel dirimere la questione, i giudici hanno ribadito invece la separazione dell'ambito di applicazione delle due discipline, sulla base del fine diverso che esse intendono perseguire. In altre parole, i giudici di Palazzo Spada hanno negato la possibilità che il diritto alla protezione dei dati personali possa sconfinare il proprio naturale ambito di applicazione e divenire rilevante per altri settori.

1.3 Decisione Facebook (B6-22/16): il rivoluzionario cambiamento d'approccio adottato dal Bundeskartellamt.

In questo contesto si inserisce la rivoluzionaria decisione assunta dall'Autorità per la concorrenza tedesca (qui di seguito *"Bundeskartellamt"*) nel febbraio del 2019[84], con la quale Facebook è stata sanzionata per abuso di posizione dominante consistente nella violazione delle norme sulla tutela dei dati personali. La decisione segna una svolta nell'evoluzione della disciplina concorrenziale, dato che

[80] AGCM, Delibera 9 febbraio 2021, accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/IP330_chiusura.pdf.
[81] Il ricorso di Facebook si basava su due elementi principali: il difetto di attribuzione dell'AGCM, dal momento che le pratiche contestate non potrebbero essere qualificate come commerciali, poiché non presuppongono il pagamento di un corrispettivo da parte dell'utente e – sorprendentemente – la considerazione che in quel caso avrebbe dovuto trovare invece applicazione la disciplina sulla tutela dei dati personali a norma del Regolamento (UE) 679/2016. Con riferimento alla prima delle due pratiche contestate (c.d. pratica a), il TAR ha rigettato l'istanza di Facebook, richiamando la dottrina dei dati come controprestazione e argomentando sulla necessità di applicare comunque le norme poste a tutela dei consumatori. Allo stesso tempo, il Tribunale amministrativo ha però escluso la sovrapponibilità della disciplina del consumo con quella relativa alla tutela dei dati personali.
[82] L'AGCM aveva contestato due diverse pratiche. La pratica a) riguardava la fase di registrazione dell'utente, durante la quale, a parere dell'Autorità, non veniva fornita un'informativa chiara sull'utilizzo dei dati, inducendo i consumatori a ritenere che il servizio fosse assolutamente gratuito. La pratica b) riguardava invece l'automatica trasmissione e l'utilizzo dei dati personali degli utenti a parte di Facebook e soggetti terzi, considerata una pratica aggressiva dal momento che veniva lasciata esclusivamente la possibilità di esercitare l'opzione *opt-out*.
[83] Consiglio di Stato sez. VI, 29 marzo 2021, n. 2630.
[84] Bundeskartellamt (n. 1).

per la prima volta la disciplina sulla tutela dei dati personali viene assunta quale parametro rilevante per accertare la violazione di una regola concorrenziale. Va preliminarmente sottolineato che la decisione si basa sulla legislazione nazionale tedesca, che di recente è stata riformata proprio nel senso di adeguare la disciplina concorrenziale alle caratteristiche dei nuovi mercati digitali, introducendo nuovi elementi che il *Bundeskartellamt* è chiamato a valutare nel corso delle indagini volte all'accertamento dell'esistenza di posizioni dominanti, fra cui il controllo esercitato sui dati[85].

La condotta sanzionata dal *Bundeskartellamt* ha ad oggetto le condizioni contrattuali imposte da Facebook sull'utilizzo dei dati acquisiti dalla piattaforma attraverso l'accesso da parte degli utenti di servizi ulteriori forniti dalla società stessa (WhatsApp, Oculus, Masquerade e Instagram) o raccolti su altri siti o *app* a cui gli utenti hanno accesso mediante i programmi di interfaccia di Facebook *("Facebook Business Tools"*). Nello specifico, viene preclusa alla società la possibilità di combinare i suddetti dati con quelli raccolti grazie all'utilizzo diretto del *social network* da parte degli utenti. La condotta abusiva, dunque, non ha ad oggetto i dati prodotti all'interno del social, quanto quelli trasmessi alla società da parte di soggetti terzi.

Preliminarmente, il *Bundeskartellamt* ha fornito un profilo completo delle attività svolte da Facebook. I servizi sviluppati e forniti sono diversi: prodotti digitali, servizi online e *app*. Il prodotto principale è costituito dal *social network* "Facebook.com", il cui accesso è subordinato alla creazione di un profilo dei singoli utenti, che presuppone la cessione di una serie di dati personali (es. nome, data e luogo di nascita, e-mail etc). Il *social network* consente agli utenti di interagire attraverso la pubblicazione di post e l'utilizzo di "Facebook Messenger" come strumento di messaggistica istantanea, nonché di accedere ad altri servizi in esso integrati. Inoltre, Facebook fornisce la possibilità di sponsorizzare prodotti, e gli effetti di tale servizio sono ottimizzati dal *"targeting"*, ossia la personalizzazione delle offerte sulla base delle preferenze manifestate da ciascun utente. A latere del *social network*, Facebook offre i *"Facebook Business Tools"*, una serie di prodotti a cui è possibile accedere gratuitamente e che vengono ingrati da soggetti terzi all'interno dei propri siti e delle proprie *app*. La società fornisce anche servizi ulteriori, attraverso altre piattaforme quali Instagram, WhatsApp, Oculus e Masquerade. Per potervi accedere, gli utenti devono accettare le *privacy* e *cookies policy* di Facebook, in virtù delle quali la società acquisisce il diritto di raccogliere ed utilizzare non soltanto i dati forniti durante l'utilizzo diretto del *social network*,

[85] La riforma introduce una nuova definizione di mercato rilevante, includendo fra gli elementi da valutare al fine di determinare se una società si trovi o meno in posizione dominante: a) l'accesso a dati rilevanti in termini concorrenziali, b) effetti *network* diretti e indiretti, c) le economie di scala della società, d) pressione competitiva guidata dall'innovazione.

ma anche quelli generati dall'utilizzo dei servizi ulteriori[86]. Il trattamento dei suddetti dati è giustificato da Facebook sulla base del legittimo interesse[87].

Al fine di determinare se la condotta tenuta da Facebook integrasse o meno una violazione della disciplina sulla concorrenza, il *Bundeskartellamt* ha anzitutto individuato il mercato rilevante, identificandolo sotto il profilo dei prodotti con quello dei *social network* e sotto il profilo geografico, invece, con il mercato nazionale tedesco[88]. Nel definire il mercato, il *Bundeskartellamt* ha analizzato i business model e la natura dei servizi forniti, qualificabili, ai sensi della legge sulla concorrenza, Sezione 18(3a) Das Gesetz gegen Wettbewerbsbeschränkungen (qui di seguito "GWB"), come prodotto intermediario, ossia una combinazione di *network* e mercato a più parti. La natura di mercato a più parti deriva in particolare dalle modalità di finanziamento del prodotto, rappresentata in misura preminente dalle sponsorizzazioni "targettizzate". Il mercato principale, ossia quello in cui opera il *social network* "Facebook.com", vede coinvolti due gruppi di utenti: i singoli individui che gratuitamente utilizzano il social e i soggetti che sponsorizzano i propri prodotti. Altri "lati" del mercato, che si aggiungono a quello principale, coinvolgono gli editori *(publishers)* che utilizzano pagine Facebook gestite da loro stessi per connettersi con gli utenti e promuovere i propri prodotti e gli sviluppatori (*developers*) che integrano Facebook all'interno dei propri siti o delle proprie *app*, utilizzando le *Application Programming Interfaces* (da qui in poi "API")[89].

Facebook è stata considerata dal *Bundeskartellamt* come dominante sul mercato sulla base di diversi elementi, primo fra tutti la quota di mercato degli utenti detenuta dalla società, stimata intorno ad una percentuale del 95%[90]. Tale percentuale va ben oltre la soglia ritenuta rilevante per l'esistenza o meno di una posizione dominante ai sensi della Sezione 18(4) GWB[91]. Anche gli effetti di rete hanno senz'altro giocato un ruolo determinante nell'acquisizione della posizione dominante di Facebook[92].

L'effetto di rete diretto più rilevante è sicuramente rappresentato dalla difficoltà per gli utenti di passare ad un *social network* diverso da Facebook. Questo ha fatto sì che diversi concorrenti uscissero dal mercato e che altri perdessero notevoli quote, entrambi sintomi non solo del fatto che Facebook si trovi

[86]Bundeskartellamt, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* (15 febbraio 2019) case summary.
[87]Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) [2016] L 119/1, art. 6, lett. f).
[88]Bundeskartellamt, (n. 1).
[89]Si tratta di interfaccia di programmazione che consentono sia l'interazione fra uomo e macchina, che la comunicazione fra diverse applicazioni. Mediante le API è dunque possibile trasferire i dati in modo ordinato, superando gli ostacoli dovuti all'eventuale utilizzo di linguaggi di programmazione diversi.
[90]Nel determinare l'effettiva posizione dei concorrenti sul mercato, si è altresì tenuto conto del tempo di utilizzo giornaliero del social network da parte degli utenti.
[91]Si tenga conto che fra i concorrenti inclusi nel mercato rilevante vi sono YouTube, Snapchat, Twitter, WhatsApp e Instagram.
[92]Giulia Schneider, "Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation Against Facebook", (2018), vol. 9/no. 4 Journal of European Competition Law & Practice, 217-218, accessibile da https://academic.oup.com/jeclap/article/9/4/213/4903311.

in una posizione dominante, ma che la stia addirittura rafforzando, divenendo un quasi-monopolista. L'effetto *network* indiretto, invece, si osserva soprattutto riguardo alla sponsorizzazione dei prodotti quale fonte di finanziamento dei servizi. Tali servizi, infatti, sono tanto più efficaci quanti più utenti riescono a raggiungere. Dal momento che Facebook detiene una quota così ampia di mercato degli utenti, per i suoi concorrenti è particolarmente difficile entrarvi e riuscire a permanervi. Combinando tutti questi elementi all'enorme quantità di dati di cui Facebook dispone, le barriere all'entrata si rafforzano drammaticamente. D'altronde, maggiore è la quantità di dati raccolti, più semplice e meno costoso è per le società produrre nuovi dati.

La disciplina tedesca sulla concorrenza, al pari di quella dell'UE, non vieta né sanziona l'esistenza *per se* di una posizione dominante, quanto l'abuso della stessa. Chi si trova in posizione dominante, infatti, è tenuto ad astenersi dal porre in essere attività che possano essere nocive per il mercato o pregiudicare in qualsiasi modo i concorrenti. Nel caso di specie, la condotta tenuta da Facebook è stata qualificata dal *Bundeskartellamt* come un abuso di sfruttamento[93] (*exploitative abuse*) secondo la disciplina concorrenziale tedesca[94]. Questa tipologia di abusi può consistere sia nell'adozione dei cosiddetti prezzi predatori[95], che, come in questo caso, nell'imposizione di clausole contrattuali inique. L'iniquità delle clausole in esame è stata determinata tenendo conto delle regole sancite dal GDPR in materia di tutela dei dati personali. Costante giurisprudenza tedesca, infatti, ha ribadito che nel valutare l'iniquità clausole contrattuali si possa fare riferimento a tutti i princìpi legali la cui *ratio* sia riconducibile alla volontà di proteggere la parte più debole in un rapporto contrattuale[96]. *Ratio* che senz'altro anima la disciplina del GDPR, volta espressamente a riequilibrare il rapporto fra i titolari del trattamento dei dati e soggetti interessati, attribuendo a questi ultimi un controllo maggiore sui propri dati personali.

Come anticipato, l'utilizzo della disciplina del GDPR quale parametro di riferimento per accertare la violazione della disciplina sulla concorrenza, rappresenta il vero punto cruciale e rivoluzionario della decisione. Nell'argomentare il proprio provvedimento, il *Bundeskartellamt* ha dunque dovuto spiegare la ragione per cui le modalità di utilizzo dei dati personali degli utenti da parte di Facebook fosse rilevante non soltanto per la disciplina sulla tutela dei dati, ma anche in termini concorrenziali[97].

---

[93] Gli abusi di sfruttamento includono quelle forme di abuso caratterizzate dal fatto che l'impresa dominante sfrutti la propria posizione per ottenere maggiori guadagni a scapito dei propri clienti. Ad esempio, l'imposizione di clausole contrattuali inique o svantaggiose è generalmente qualificata proprio come un abuso di sfruttamento.

[94] Germania, *GWB,* Section 19(1).

[95] Con l'espressione "prezzi predatori" si fa riferimento alla pratica commerciale consistente nel rivendere beni o servizi a prezzi più bassi dei costi marginali. Sebbene questo avvantaggi nel breve periodo i consumatori, che avranno accesso a quei prodotti a prezzi vantaggiosi, determina un pericolo per il mercato, poiché si tratta di una condotta insostenibile per i concorrenti, che saranno costretti ad uscire dal mercato stesso.

[96] Bundeskartellamt, *Background information on the Facebook proceeding,* (19 dicembre 2018), accessibile da https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf;jsessionid=23A62F7CF5798330201105AA27D28631.1_cid362?__blob=publicationFile&v=6.

[97] Bundeskartellamt, (n. 1).

I social network – ha spiegato il *Bundeskartellamt* – sono servizi *data-driven*. Ciò vuol dire che l'accesso e l'utilizzo dei dati assumono un'importanza centrale nel determinare la posizione sul mercato delle società che forniscono tali servizi. Data tale correlazione, è dunque compito delle autorità garanti della concorrenza vigilare sulle modalità con cui l'accesso avviene ed indagarne le possibili conseguenze in termini concorrenziali, tenendo conto, nel corso delle proprie indagini, anche dei princìpi legali dettati in materia di protezione dei dati. Il cambiamento di approccio è legato ad una profonda riflessione sulle caratteristiche del business model adottato da Facebook e, più in generale, dalle piattaforme digitali, in cui la centralità assunta dei dati è tale per cui, volendo comprendere quali siano realmente le dinamiche di mercato e la forza di ciascun *player* al suo interno, non si può assolutamente prescindere dall'assumere questi ultimi quali elementi di valutazione. Questo non vuol dire che il Bundeskartellamt sia compente nel verificare se le condizioni contrattuali violino o meno la disciplina del GDPR, ma soltanto che questa viene assunta quale parametro di riferimento ai fini delle indagini sulla violazione delle regole sulla concorrenza[98].

L'autorità tedesca è giunta dunque alla conclusione che le condizioni imposte dalle *privacy policy* adottate da Facebook costituisse una violazione del GDPR, con riferimento alle modalità di trattamento dei dati acquisiti grazie all'interazione con soggetti terzi (mediante le API) o attraverso i servizi ulteriori erogati dalla società (es. WhatsApp e Instagram), in quanto il trattamento non sarebbe adeguatamente sostenuto da nessuna delle basi giuridiche indicate dal GDPR. Il Bundeskartellamt ha infatti sottolineato che, in ragione della posizione dominante detenuta da Facebook sul mercato, il consenso prestato dagli utenti ai termini e alle condizioni proposte dalla società, al solo fine di concludere il contratto, non potesse dirsi libero ai sensi dell'art. 6(1a) GDPR. Al contempo, il *Bundeskartellamt* esclude che il trattamento dei dati sia giustificato alla luce di una delle altre basi giuridiche[99] ed in particolare del legittimo interesse, essendo necessario un bilanciamento fra quest'ultimo e gli interessi degli altri soggetti convolti, compresi gli utenti e le terze parti[100]. Tenuto conto della tipologia dei dati raccolti, delle modalità di trattamento, delle ragionevoli aspettative degli utenti e della loro posizione rispetto alla società, il *Bundeskartellamt* ritiene infatti che neanche il legittimo interesse sia idoneo a giustificare il trattamento.

Sebbene gli utenti non soffrano di un danno economico diretto, dal momento che i servizi vengono erogati loro gratuitamente, questi soffrono comunque un pregiudizio in termini di perdita di controllo sul trattamento dei propri dati personali, possibile in virtù dello squilibrio di potere contrattuale fra le parti[101]. In altri termini, affermando l'esistenza di una correlazione fra l'iniquità delle condizioni contrattuali e la violazione della disciplina del GDPR, il *Bundeskartellamt* ha stabilito da un lato che la

[98] Bundeskartellamt, (n. 86).
[99] GDPR, art. 6.
[100] Bundeskartellamt, (n. 88).
[101] Bundeskartellamt, (n. 1).

raccolta di dati personali consente di acquisire potere sul mercato e dall'altro, che qualora questa avvenga in maniera illegittima, possa comprometterne l'equilibrio, a danno sia dei concorrenti che dei consumatori[102].

Compreso l'iter decisionale seguìto dall'Autorità tedesca e ferma l'indiscussa importanza che questa riveste quantomeno nell'indicare che a livello nazionale è già in atto un cambiamento di passo sul fronte dell'integrazione fra la disciplina concorrenziale e la tutela dei dati personali, resta da chiedersi quale sarà l'impatto che questa potrà avere a livello europeo. A tal proposito, la questione è stata rinviata in via pregiudiziale alla CGUE[103], la quale sarà chiamata a valutare la validità della decisione.

Una primissima considerazione può farsi guardando alla lettera dell'art. 102 TFUE che, limitandosi ad un generale riferimento a "pratiche commerciali scorrette", apre alla necessità di integrazione della stessa con altre branche del diritto al fine di definire la portata sostanziale della norma[104]. Indagando ad esempio sui punti di contatto fra la disciplina concorrenziale e quella relativa alla tutela dei consumatori, ci si è interrogati sull'opportunità di identificare il danno sofferto dai consumatori in termini non economici. Tradizionalmente si riteneva che il benessere del consumatore coincidesse esclusivamente con il miglior rapporto prezzo/output[105]. Di recente, invece, si è osservato che se questo è vero nel breve periodo, nel medio e nel lungo termine è necessario valutare anche fattori ulteriori, quali la qualità, la varietà e l'innovazione dei prodotti.

Bisogna chiedersi se le *privacy policy* adottate dalla società possano essere effettivamente qualificate come condizioni contrattuali e se pertanto la loro illegittimità sia sufficiente a renderle inique secondo i criteri dettati dall'art. 102 TFUE. Come sottolineato dal Bundeskartellamt nella propria decisione, nel *business model* adottato da Facebook i dati personali forniti dagli utenti rappresentano di fatto il corrispettivo pagato da questi ultimi per avere accesso ai servizi. Le *privacy policy* dettano dunque le regole contrattuali volte a disciplinare il rapporto fra gli utenti e la società. In quest'ottica, non vi è ragione di negare che queste ricadano nell'ambito di applicazione dell'art. 102 TFUE e che possano essere qualificate come condizioni commerciali. Né tantomeno, alla luce della costante giurisprudenza europea[106], sembrerebbero porsi dubbi circa la violazione della disciplina concorrenziale sia determinata dalla violazione di disposizioni relative ad altri settori.

Ad esempio, la CGUE ha stabilito[107] che, a certe condizioni, la violazione delle norme sulla proprietà intellettuale può essere rilevante in ambito concorrenziale. Non vi è pertanto motivo di escludere che il

[102]Ibid.
[103]Causa C-319/20 *Domanda di pronuncia pregiudiziale proposta dal Bundesgerichtshof (Germania) — Facebook Ireland Limited / Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V.* [2020] C 359/2.
[104]Bundeskartellamt, (n. 1).
[105]Ibid. Sul punto si richiama anche quanto detto sopra a proposito della strategia commerciale adottata da Amazon.
[106]Vedi Caso C-32/11 *Allianz Ungheria* [2013] C 141/3.
[107]Vedi C-457/10 *AstraZeneca AB and AstraZeneca plc v European Commission* [2012].

medesimo principio possa trovare applicazione con riguardo alle norme sulla tutela dei dati personali. È, d'altronde, quello a cui lo European Data Protection Board (da qui in poi "EDPB") ha fatto riferimento suggerendo la necessità di adottare un "approccio olistico" nell'attuazione della disciplina sulla tutela dei dati personali[108], ossia favorendo una maggiore cooperazione fra le autorità competenti in questo settore, con le omonime operanti nell'ambito della tutela dei consumatori e della concorrenza. L'EDPB ha infatti sottolineato che in un mercato in cui il potere è acquisito grazie all'accesso ai dati personali, la tutela dei dati personali diviene senza dubbio un vantaggio competitivo.

A questo punto, bisogna chiedersi quali siano le condizioni necessarie affinché la violazione di norme sulla tutela dei dati personali possa altresì costituire un abuso di posizione dominante. Le condizioni contrattuali saranno considerate inique nella misura in cui non possiedano i requisiti di proporzionalità, necessità e trasparenza[109]. In altri termini, dovrà valutarsi se le limitazioni sul controllo degli utenti sui propri dati personali siano proporzionali e necessarie al fine di consentire l'accesso al servizio e se le condizioni stabilite dalle *policy* siano comunicate in modo sufficientemente chiaro e non inducano in errore la controparte. Sotto questo punto di vista si può osservare che i princìpi alla luce dei quali è valutata la legittimità delle clausole contrattuali coincidano di fatto con le condizioni di legittimità dettate dalla disciplina sulla tutela dei dati personali. Come già detto, tuttavia, ciò non comporta che ogni violazione delle regole sulla protezione dei dati personali si traduca automaticamente in una violazione delle regole sulla concorrenza[110]. Affinchè possa effettivamente essere stabilita l'esistenza di un nesso fra le due discipline, infatti, è necessario verificare un elemento ulteriore: se, cioè, l'adozione di condizioni contrattuali inique dipenda dalla posizione dominante della società. Nel caso di Facebook, come ampiamente illustrato sopra, l'esistenza di un nesso fra le due circostanze è chiara ed è stata ben mostrata dal *Bundeskartellamt*.

Almeno a livello europeo, la strada sembra ormai essere stata segnata, e lo dimostrano non soltanto le nuove proposte di Regolamento presentate della Commissione[111], ma anche le più recenti istruttorie iniziate da quest'ultima. Il caso che sta facendo discutere maggiormente riguarda Apple[112], al momento nel mirino di due diverse indagini, riguardanti rispettivamente Apple Pay ad Apple Store.

Dopo le obiezioni sollevate da alcuni concorrenti della società, fra cui in particolare Facebook, si è deciso di indagare sulle reali conseguenze del cambiamento apportato da Apple alle condizioni dettate dalle proprie *privacy policy*. La Commissaria Vestager ha dichiarato che, nonostante le nuove misure

[108]Schneider, (n. 92), 216.
[109]Ibid, 222.
[110]Ibid, 224.
[111]Vedi note 4 e 5.
[112]Laura Liguori, Enzo Masarà, "Quel braccio di ferro fra privacy e concorrenza dietro il caso Apple", Wired (17 marzo 2021), accessibile da https://www.wired.it/economia/business/2021/03/17/apple-privacy-concorrenza-antitrust/ e Foo Yun Chee, "Exclusive: EU's Vestager warns Apple to treat all apps equally amid privacy dispute", Reuters (8 Febbraio 2021), accessibile da https://www.reuters.com/article/idUSL1N2KE243.

adottate sembrerebbero attribuire agli utenti maggior controllo sui propri dati personali, potrebbe comunque configurarsi un abuso di posizione dominante se venisse dimostrato che le *app* proprie di Apple siano soggette ad un trattamento diverso e più vantaggioso rispetto alle altre. Entrando più nello specifico, Apple ha modificato le condizioni relative al tracciamento dei dati degli utenti che utilizzano le *app* sui propri dispositivi, prevedendo come impostazione di default che il tracciamento dei dati sia disattivato e possa essere attivato solo dall'utente stesso, esprimendo il proprio esplicito consenso. La Commissaria stessa ha manifestato apprezzamento verso la scelta di introdurre un meccanismo *out-opt*, che restituisce al soggetto interessato un effettivo controllo sui propri dati, nello spirito del GDPR.

Ciò che viene contestato dai concorrenti, chiaramente danneggiati da un'opzione che rende molto meno proficuo sponsorizzare i propri prodotti attraverso i dispositivi Apple, è che in tal modo le *app* della società stessa si troverebbero in una posizione di vantaggio, sia perché queste sfruttano sistemi di tracciamento non toccati dalla riforma, sia perché il sistema iOS è un sistema chiuso, che non consente la commercializzazione delle *app* al di fuori di Apple Store. Il caso dimostra che la tutela dei dati personali è ormai riconosciuta come elemento concorrenziale rilevante e che ci si sta muovendo verso una convergenza sempre maggiore fra le due discipline.

1.4 La regolamentazione dei dati: dal GDPR alle nuove proposte della Commissione.

Alla luce delle riflessioni e delle analisi svolte nei paragrafi precedenti, è facile comprendere le ragioni per cui il legislatore europeo si sta muovendo, già da diversi anni, nel senso di promuovere lo sviluppo di un *frame work* normativo omogeneo su tutto il territorio degli Stati Membri per regolare la circolazione dei dati sia personali che no. Lo scopo è quello di consentire alle imprese di restare competitive sia dentro che fuori il mercato interno, senza frenare lo sviluppo della tecnologia e l'innovazione.

Le iniziative intraprese in tal senso sono molteplici e lo stesso GDPR, nato per promuovere la libera circolazione dei dati personali, conciliando la tutela di diritti fondamentali alle esigenze di natura economica, si inserisce perfettamente in questo contesto. Il GDPR è dichiaratamente "neutro" rispetto alle tecnologie[113], confermando la volontà del legislatore europeo non soltanto di fornire alle imprese strumenti in grado di sopravvivere all'evoluzione tecnologica ma, anzi, di guidarla su percorsi compatibili con i principi fondamentali dell'ordinamento europeo.

[113]GDPR, considerando 15 "Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. […]"

Per fornire un quadro completo delle iniziative legislative intraprese a livello europeo in tal senso, deve farsi menzione anche del Cybersecurity Act[114], dell'Open Data Directive[115] e della e-Privacy Directive[116]. Il primo è volto alla creazione di standard di sicurezza uniformi sul tutto il territorio dell'Unione Europea, promuovendo la cooperazione fra gli enti nazionali competenti per la sicurezza e l'European Union Agency for Network and Innovation Security (qui di seguito "ENISA") per la diffusione delle *best practises* per la condivisione sicura dei dati. La seconda regola invece la circolazione dei dati prodotti dalle Pubbliche Amministrazioni, mentre la terza, che dovrebbe essere sostituita a breve dall'e-Privacy Regulation[117], ha ad oggetto la tutela della vita privata e dei dati personali nelle comunicazioni elettroniche.

Diverse sono le premesse a questo percorso di iniziative legislative. Il primo passo è stato senza dubbio riconoscere il valore economico dei dati. Definendo questi ultimi come "la materia prima dei *business model* digitali"[118], infatti, l'EDPS ha dimostrato di aver colto pienamente la centralità assunta dai dati nelle moderne strutture di mercato. I dati vengono finalmente intesi come vera e propria controprestazione dei servizi offerti sulle piattaforme digitali, e nella proposta di una Direttiva per la regolamentazione dei contratti digitali[119], la Commissione si era spinta fino ad ipotizzarne la piena equiparazione alla valuta, riconoscendoli come mezzo di pagamento[120].

Partendo da questa considerazione, viene sostenuta la necessità di rendere gli individui maggiormente consapevoli del valore dei propri dati, attribuendo loro più controllo su di essi. Si ritiene, infatti, che ciò si tradurrebbe in una maggiore attenzione sull'utilizzo che ne viene fatto e sulla cessione a soggetti terzi. Oltre ad attribuire ai soggetti interessati maggior controllo, dunque, si dovrebbero fornire loro adeguate e complete informazioni sull'utilizzo – effettivo e potenziale – che può essere fatto dei loro dati personali. Uno dei fattori che contribuisce a far sì che i dati personali continuino ad essere sfruttati economicamente, infatti, è la forte asimmetria informativa che caratterizza i rapporti contrattuali fra gli utenti e le grandi piattaforme. Per far fronte a questo problema, con l'adozione del GDPR ci si è mossi nel senso di garantire agli individui uno specifico diritto di informazione[121].

---

[114]Regolamento (UE) 881/2019 del Parlamento Europeo e del Consiglio del 17 Aprile 2019 relativo all'ENISA, l'Agenzia l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cybersicurezza»), [2019] OJ L 151.
[115]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 [2019] OJ L. 172/56.
[116] Direttiva del Parlamento Europeo e del Consiglio 2002/58/EC del 12 Luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata del settore delle comunicazioni elettroniche [2002] OJ L. 201/37.
[117] Commissione, Proposta di Regolamento del Parlamento Europeo e del Consiglio del 10 gennaio 2017 relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE [2017].
[118]EDPS, *Opinion on coherent enforcement of fundamental rights in the age of big data,* Opinion 8/2016, https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.
[119]Commissione, Proposta per una Direttiva del Parlamento europeo e del Consiglio su certi aspetti concernenti i contratti per la fornitura di servizi digitali, COM (2015) 634, https://ec.europa.eu/transparency/regdoc/rep/1/2015/IT/1-2015-634-IT-F1-1.PDF.
[120]EDPS, "Privacy and competitiveness in the age of big data", (n. 77).
[121]GDPR, art. 12.

La proposta della Commissione mirava però oltre, attribuendo loro la possibilità di scegliere se pagare un determinato servizio mediante la cessione dei propri dati personali o in denaro. Si passerebbe così dal concepire l'utente come un soggetto debole, ad attribuirgli un ruolo attivo all'interno del mercato. Questa visione "antropocentrica" è stata adottata anche più di recente nell'ambito delle successive riflessioni sullo sviluppo dell'AI[122].

Naturalmente, però, ciò sarebbe possibile solo nella misura in cui vi siano dei criteri che consentano di determinare chiaramente e in modo oggettivo quanto valgono i dati. Le soluzioni potrebbero essere due[123]. Adottando un approccio *top-down*, il valore dei dati potrebbe essere determinato calcolando quale sia il fatturato maturato dalle imprese grazie all'utilizzo delle sponsorizzazioni personalizzate. Guardando invece al valore dei dati in una prospettiva *bottom-down* (cioè dal punto di vista degli utenti), il loro valore andrebbe commisurato al danno sofferto in ragione della perdita della tutela dei propri dati e della maggiore asimmetria contrattuale. In entrambi i casi, il valore accertato sarebbe comunque approssimativo e, soprattutto, rimane aperto il dubbio sul soggetto a cui spetterebbe il compito di determinarlo. Inoltre, attribuire agli individui la facoltà di scegliere se pagare utilizzando i propri dati personali o la valuta corrente potrebbe porsi in contrasto con alcuni dei princìpi sanciti dal GDPR, specie - come si vedrà meglio di seguito - in materia di consenso.

L'esigenza di costruire un *frame work* normativo in grado di accompagnare il progresso tecnologico verso una direzione *privacy-friendly* si era manifestata a livello internazionale già molto prima dell'entrata in vigore del GDPR, sin dagli anni '80, quando l'Organization for Economic Coperation and Development (da qui in poi "OECD") ha elaborato e pubblicato interessanti linee-guida in materia di privacy[124], nelle quali l'organizzazione aveva enucleato principi fondamentali molto vicini a quelli poi successivamente confluiti nel GDPR.

Proprio con riferimento a tali principi, erano sorte delle riflessioni sui rischi posti dall'avvento delle nuove tecnologie e, nello specifico, non solo per quelli legati allo scambio e alla diffusione di grandi quantità di dati, ma anche e soprattutto delle difficoltà riconducibili al loro possibile riutilizzo e all'imprevedibilità del valore che se ne può trarre[125], auspicando un ripensamento dei suddetti princìpi, che tenesse conto delle nuove esigenze emergenti. Guardando al problema da un diverso punto di vista,

---

[122] Sul punto si veda diffusamente Gruppo di esperti del MISE sull'Intelligenza Artificiale, *Proposte per una strategia italiana sull'Intelligenza Artificiale,* (2020), accessibile da https://www.mise.gov.it/index.php/it/198-notizie-stampa/2041246-intelligenza-artificiale-online-la-strategia.

[123] Gianclaudio Malgieri, Bart Custers, "Pricing Privacy – the Right to Know the Value of Your Personal Data", (2018), vol. 34/no. 2 The Computer Law and Security Report, 291, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917302819?via%3Dihub.

[124] Organization for Economic Co-operation development (OECD), *Guidelines governing the protection of privacy and transborder flows of personal data*, Annex to the Recommendation of the Council of 23th September 1980, (1980). Le linee-guide includono infatti il principio di limitazione della raccolta e nell'utilizzo dei dati, di qualità degli stessi, di specificazione della finalità, di sicurezza.

[125] F. H. Cate e Viktor Mayer-Schonberger, "Notice and Consent in a World of Big Data", (2013), vol. 3/no. 2 International Data Privacy Law, 67, accessibile da https://academic.oup.com/idpl/article/3/2/67/709124.

va inoltre considerato che il rispetto della stringente disciplina dettata dal GDPR precluderebbe la possibilità di trattare una parte di dati invece molto rilevanti per il buon funzionamento dei nuovi sistemi[126]. La tensione fra la tutela dei dati e lo sviluppo delle nuove tecnologie, dunque, è altissima.

1.4.1 Big Data e GDPR

I temi che emergono nell'ambito dell'analisi del GDPR alla luce del fenomeno dei Big Data sono molteplici ed ognuno di essi assume una diversa declinazione nel contesto specifico delle singole tecnologie che sono interessate da questo fenomeno e il cui sviluppo è direttamente ricollegato proprio all'analisi dei dati, fra cui ad esempio i sistemi IoT e la *blockchain*.

a) La "privacy di gruppo"

L'ambito d'applicazione del GDPR è limitato al trattamento sia automatizzato che no dei dati personali delle persone fisiche[127]. Per trattamento dei dati s'intende qualunque azione compiuta su di essi, spaziando dalla semplice lettura alla loro analisi ed elaborazione. La distinzione fra dati personali e no è però resa sempre più complessa dallo sviluppo delle nuove tecnologie. La definizione di "dato personale" fornita dal GDPR fa riferimento in senso soggettivo ad una persona fisica determinata, mentre da un punto di vista oggettivo guarda alla capacità dei dati di consentirne l'identificazione. Ogni qualvolta si possa parlare di Big Data, vengono invece in rilievo problemi che affliggono il gruppo e non il singolo[128]. Le decisioni assunte hanno un impatto sull'individuo non perché venga data rilevanza al singolo in quanto tale, quanto piuttosto per la sua appartenenza ad un determinato gruppo.

Sin dall'adozione della Direttiva 95/46/EC che, fino all'entrata in vigore del GDPR, ha regolato a livello europeo la protezione dei dati personali, si è mantenuta l'equivalenza soggetto interessato/persona fisica, anche se alcune disposizioni aprivano già alla possibilità di tenere in considerazione i rischi in cui il singolo si sarebbe potuto imbattere per la propria appartenenza ad un determinato gruppo (es. discriminazioni in ragione della propria origine etnica o razziale). Il GDPR ha introdotto delle novità sotto questo profilo, riconoscendo ai soggetti interessati il diritto di conferire mandato ad un organismo no profit, ad un'organizzazione o associazione per la tutela collettiva dei propri interessi, giungendo addirittura a riconoscere a questi ultimi il potere di sporgere reclamo anche in assenza di un espresso

[126] Nishtha Madaan, Mohd Abdul Ahad, e Sunil M. Sastry, 'Data Integration in IoT Ecosystem: Information Linkage as a Privacy Threat', (2018), vol. 34/no. 1 The Computer Law and Security Report, 126, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917301358?via%3Dihub.

[127] GDPR, art. 2, comma 1.

[128] Ugo Pappagallo, Massimo Durante, Shara Monteleone, "What is new with the Internet of things in privacy and data protection? Four legal challenges on sharing and control in IoT" in Hert, Paul De, Serge Gutwirth, Rosamunde van Brakel, and Ronald Leenes *Data Protection and Privacy: (in)Visibilities and Infrastructures*, (2017), Springer International Publishing, 67.

mandato da parte dell'interessato. In questo modo, tuttavia, il legislatore europeo non ha inteso stravolgere l'impostazione originaria del diritto alla tutela dei dati personali, ma ha ritenuto ragionevole riconoscere ai rappresentanti di uno specifico gruppo il potere di agire di fronte alle autorità competenti ogni qualvolta la violazione della disciplina sui dati personali si traducesse in un danno proprio per quel gruppo.

La definizione di "privacy del gruppo" può essere data seguendo due diversi approcci[129]. Da un lato, questa potrebbe essere definita come la privacy relativa alle informazioni condivise all'interno di un gruppo da parte dei suoi membri. Questa definizione non consente tuttavia di riconoscere la privacy del gruppo come elemento autonomo, ma soltanto come una delle possibili inclinazioni della privacy individuale. Il secondo approccio, invece, guarda al gruppo come ad un'entità autonoma, e non come la somma delle singole individualità. Ciò consente di cogliere più chiaramente i pericoli a cui il gruppo è esposto e la direzione verso cui dovrebbe muovere la legislazione. È proprio in virtù delle tipologie di algoritmi utilizzati che vengono infatti individuate le più disparate correlazioni fra gli individui, creando, sulla base di caratteristiche comuni, gruppi a cui i singoli non sono neanche consapevoli di appartenere. Gli individui non hanno dunque conoscenza di chi siano gli altri membri del gruppo, né piena consapevolezza dei rischi in cui incorrono. Si tratta inoltre di classificazioni di natura variabile, e non è raro che un individuo dapprima inserito in un determinato gruppo, sia successivamente riconosciuto come appartenente ad un altro.

I danni a cui gli individui sono potenzialmente esposti, dunque, si amplificano, includendo anche i rischi legati a trattamenti discriminatori[130] ed invasivi. L'accuratezza dei dati diventa dunque elemento imprescindibile al fine di garantire la correttezza, la legittimità e la giustizia dei processi decisionali elaborati e di cui i dati costituiscono la base. La disciplina è inadeguata a tutelare effettivamente i soggetti esposti a questi rischi, dal momento che pone quale condizione preliminare per la propria applicabilità che il trattamento riguardi dati grazie ai quali è possibile l'identificazione di un soggetto determinato[131].

Quello di cui si sta trattando è un profilo che rileva con riguardo al cosiddetto "utilizzo etico" dei dati, di cui si molto discusso proprio in ragione dell'evoluzione dell'AI[132]. Ogni errore nella formazione degli

---

[129] Alessandro Mantelero, "Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection", (2016), vol. 32/no. 2 The Computer Law and Security Report, 238-255, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364916300280?via%3Dihub.

[130] Il concetto di discriminazione può essere definito sia in senso negativo che positivo. In senso negativo, questa consiste nel trattamento ingiusto o pregiudizievole di categorie diverse, mentre nella sua accezione positiva, implica soltanto il riconoscimento e la comprensione delle differenze fra due soggetti. Se da un lato il trattamento differenziato di situazioni fra loro distinte è perfettamente compatibile con il principio di uguaglianza sostanziale che, non solo permea l'intera disciplina europea, ma assurge al ruolo di principio fondamentale anche a livello internazionale, è vero anche che una rappresentazione distorta della realtà sulla base dei dati raccolti, può comportare discriminazioni in senso negativo.

[131] Prof. Dr. Lilian Mitrou, "Is the general data protection Regulation (GDPR) 'artificial-intelligence proof?", (2018), accessibile da https://ssrn.com/abstract=3386914 ,43-44.

[132] Gruppo di esperti del MISE sull'Intelligenza Artificiale, (n. 122), 54-55; European Commission, *White Paper On Artificial Intelligence - A European approach to excellence and trust*, COM(2020) 65 final.

algoritmi, che rispecchi pregiudizi o errori propri della valutazione umana, è destinato ad avere un impatto devastante, perché replicato su larga scala e dunque enfatizzato ed assunto quale criterio determinante su cui basare decisioni rilevanti. Questo è tanto più vero se si tiene conto delle tipologie di algoritmi che vengono impiegati a tal fine, in generale riconducibili a due categorie: 1) gli algoritmi predittivi o *analytics* che consentono di anticipare le scelte degli individui, analizzandone il comportamento; 2) gli algoritmi *machine learning*, che consentono al sistema informatico di migliorare le proprie prestazioni, imparando dall'esperienza pregressa[133].

b) L'identificazione del soggetto

Stando alla lettera del GDPR, affinché un dato possa essere qualificato come personale è necessario che questo consenta l'identificazione di un soggetto specifico. Di contro, l'applicazione del GDPR è esclusa quando i dati possono essere qualificati come anonimi, posto che si la re-identificazione divenga impossibile in maniera irreversibile. Stando alle linee-guida sull'anonimizzazione e la pseudonimizzazione emanate nel 2014 dall' Article 29 Working Party (da qui in poi "Art. 29 WP")[134], l'identificazione del soggetto si ha in tre ipotesi: 1) quando attraverso i dati è possibile *individuare* un soggetto, 2) quando è possibile *collegare* fra loro dati riferiti al medesimo soggetto e 3) quando informazioni riguardanti un soggetto possono essere *dedotte* a partire dai dati.

Le tecniche di anonimizzazione dei dati sono molteplici e l'irreversibilità dell'azione dovrà valutarsi tenendo conto dell'evoluzione della tecnologia[135]. Non rileva quali siano le intenzioni del titolare o del responsabile del trattamento, ma soltanto che, sulla base della tecnologia disponibile, l'identificazione sia possibile[136]. Viene espressamente chiarito che i dati raccolti per finalità statistica sono esclusi dall'ambito di applicazione della disciplina, dal momento che si tratta di dati aggregati che non vengono trattati al fine di assumere decisioni rilevanti per un singolo individuo e a partire dei quali il soggetto non può essere identificato.

E' dunque di fondamentale importanza stabilire se attraverso determinati dati sia possibile identificare un soggetto, perché da tale circostanza consegue l'applicazione o meno della disciplina sulla tutela dei dati personali e, di conseguenza, di un diverso livello di tutela dell'interessato. Tuttavia, la raccolta enormi moli di dati e, soprattutto, l'utilizzo delle tecniche di analisi degli stessi, pongono non pochi

[133]AGCM, AGCOM, GPDP, (n. 8), 24.
[134]Art 29 WP, *Opinion 05/2014 on anonymization tecnhiques*, 0829/14/EN. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.
[135]European Union Agency for Fundamental Rights (da qui in poi "FRA"), European Court of Human Rights (da qui in poi "ECHR"), Council of Europe (da qui in poi "CoE"), "Handbook on European data protection handbook", 2018, 93-94.
[136] Prof. Dr. Mitrou, Lilian, (n. 131), 30.

problemi nel determinare con certezza se i dati possano o meno consentire l'identificazione di un soggetto[137].

Da un lato, infatti, è possibile che certi dati, irrilevanti se guardati singolarmente, assumano un significato diverso quando correlati ad altri. Questo concetto, d'altronde, è già stato analizzato con riferimento all'attività svolta dalle piattaforme digitali, le quali sono in grado di perfezionare i servizi di sponsorizzazione offerti proprio in ragione della maggiore accuratezza dei profili degli utenti, determinata dalla possibilità di combinare un numero maggiore di informazioni, contenute in diversi *datasets*. Dall'altro lato, un significato ulteriore può essere attribuito ai dati dagli stessi algoritmi, specialmente i *machine learning* che, sulla base dell'esperienza e dell'analisi continua dei dati, sono in grado di giungere a conclusioni inizialmente neanche prevedibili, secondo meccanismi difficili da comprendere anche per coloro che li hanno sviluppati.

Si è giunti addirittura a sostenere che, tenendo conto dell'evoluzione attuale della tecnologia, non è più possibile ritenere i dati anonimi in maniera irreversibile, rendendosi così necessario adottare una nozione più ampia di dati personali, tale da includere praticamente la totalità dei dati raccolti[138]. Dal momento che, almeno potenzialmente, qualunque dato può di fatto condurre all'identificazione di un soggetto, si ritiene opportuno estendere la tutela accordata dal GDPR a tutti i dati. L'espressione "qualunque informazione", infatti, fa passare in secondo piano la natura dell'informazione, né viene data rilevanza al suo contenuto o alla forma in cui è trasmessa. Un dato costituisce un'informazione quando è possibile attribuire ad esso uno specifico significato. La possibilità di qualificare o meno un dato come informazione dipende dunque dal soggetto destinatario. A fronte della limitata capacità umana di attribuire significato ai dati, macchine e computer sono in grado di elaborare i dati in modo molto più significativo e l'impiego crescente di algoritmi sempre più sofisticati fa sì che tutti i dati diventino di fatto delle informazioni.

Il GDPR definisce i dati personali utilizzando l'espressione "riferiti a" una persona fisica identificata o identificabile. Questa espressione ha un significato più ampio di quello di dati "riguardanti" una persona, poiché vi include anche i dati utilizzati allo scopo di valutare, trattare in un determinato modo o influenzare il comportamento di un soggetto, così come quelli che possono avere un impatto sui diritti e gli interessi di quest'ultimo. E ciò non soltanto quando i dati sono effettivamente usati in tal senso, ma

---

[137] Alessandro Mantelero e Giuseppe Vaciago, "Internet of things (IoT)" in Panetta, Antonio, Augusta Iannini, Guido Alpa, Stefano Rodotà, S. Rodotà, and G. Alpa *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)*, (Milano: Giuffrè Francis Lefebvre, 2019), 562-566.

[138] Sandra Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", (2018), Vol. 34 no. 3 *The Computer Law and Security Report* 34, 443, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917303904?via%3Dihub; si veda diffusamente Nadezhda Purtova, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law", (2018) *vol. 10/no. 1 Law, Innovation and Technology,* accessibile da https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176.

anche quando potrebbero esserlo solo potenzialmente. Tuttavia, la CGUE ha più volte abbracciato un'interpretazione non troppo estensiva della nozione di dato personale[139], stressando l'importanza del principio di proporzionalità nell'applicazione del diritto dell'UE, ma, al tempo stesso, ampliando il novero dei soggetti tenuti a garantire il rispetto della disciplina.

In effetti, adottare una nozione eccessivamente ampia di dato personale, dilatando a dismisura l'ambito di applicazione del GDPR, finirebbe con l'inficiare l'effettività delle misure ivi previste. Fra le soluzioni prospettate vi sono quella di prevedere misure diverse a seconda della tipologia di dati personali oppure sulla base del grado di identificabilità della persona da questi consentito[140]. Questa ipotesi incontra però dei limiti, dal momento che si tratta parametri difficili da determinare con certezza. Più drastica è invece la posizione assunta da chi sostiene che i limiti sin qui esaminati possano superarsi soltanto abbandonando la distinzione fra dati personali e non come elemento imprescindibile per l'applicazione delle regole sulla protezione dei dati personali, favorendo piuttosto un approccio volto a valutare caso per caso quali rischi siano legati al trattamento di qualunque tipo di dato. La direzione avallata maggiormente a livello istituzionale è quella di passare dall'attuale approccio *risk-based* ad un approccio *zero-risk*, inteso però nel senso di chiedersi se la re-identificazione sia o meno "ragionevolmente possibile"[141]. Non mancano però critiche rivolte anche a questa tesi, tacciata di essere idealistica e non praticabile.

La possibilità di combinare fra loro diversi *datasets* e di analizzare i dati disponibili con tecniche particolarmente sofisticate è problematica anche nella misura in cui consentirebbe al titolare del trattamento di trarre dati personali appartenenti a categorie speciali ai sensi dell'art. 9 del GDPR (es. dati sulla salute, sull'orientamento sessuale, sull'origine etnica etc.) pur partendo dal trattamento di altre categorie. La norma infatti impone al titolare del trattamento di garantire livelli di tutela superiore rispetto a quelli ordinari ma, dal momento che i suddetti dati potrebbero essere ricavati in una fase soltanto avanzata del trattamento, ne seguirebbe l'assoluta impossibilità di adempiere ai suddetti obblighi – ivi compresi gli obblighi di informazione nei confronti del soggetto interessato – nel momento in cui i dati vengono raccolti.

c) I princìpi generali e i diritti dell'interessato

[139] Case C- 582/14 *Patrick Breyer c. Bundesrepublik Deutschland* [2016]; Case C-434/16 *Peter Nowak c. Data Protection Commissioner* [2017]; C-141/12 *YS e altri c. Minister voor Immigratie, Integratie en Asiel* [2014].
[140] Purtova (n. 138), 79-80.
[141] European Parliamentary Research Service (da qui in poi "EPRS"), "Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?" (2019), accessibile da https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf, 20.

Lo sfruttamento economico dei dati impone altresì delle riflessioni relative al rispetto dei principi dettati dall'art. 5 del GDPR, di cui dev'essere assicurato il rispetto ogni qualvolta venga posto in essere il trattamento dei dati personali.

Il principio di liceità

Tra i principi più importanti vi è certamente quello di liceità[142], in virtù del quale il trattamento dei dati personali potrà dirsi legittimo soltanto qualora avvenga nel pieno rispetto di tutte le disposizioni di legge. A questo principio è correlata la necessaria individuazione di una delle basi giuridiche elencate dall'art. 6 del GDPR che giustifichi il trattamento dei dati. Fra queste, è riconosciuta centrale importanza al consenso[143], alla luce della *ratio* generale, ossia garantire al soggetto interessato pieno controllo sui propri dati personali. A tal fine è richiesto che il soggetto sia posto nelle condizioni di fornire il proprio consenso in modo libero, specifico ed informato. Solo il rispetto di questi tre requisiti, come ribadito anche dalle più recenti linee-guida dell'EDPB[144], fa sì che questo possa dirsi pienamente valido. Nel documento vengono chiariti la portata e il significato da attribuire nel concreto ai suddetti requisiti e, analizzando le considerazioni ivi elaborate, emergono non poche preoccupazioni sull'effettiva conciliabilità del sistema normativo vigente con l'impiego di nuove tecnologie.

Affinché il consenso possa dirsi liberamente dato, bisognerà in primo luogo tenere conto dello squilibrio di potere fra le parti, ossia titolare del trattamento e soggetto interessato. Nel caso delle grandi piattaforme è facile immaginare situazioni in cui l'interessato si trovi in una posizione di debolezza rispetto al titolare del trattamento[145]. Secondo quanto stabilito dalle linee-guida dell'EDPB, il soggetto interessato dovrà essere in grado di effettuare una scelta reale, senza incorrere in alcun rischio di intimidazione, coercizione o conseguenze negative, che possono consistere anche nel pagamento di costi extra[146].

Nella proposta che ha preceduto l'adozione della Direttiva sulla fornitura di servizi digitali[147], che s'inserisce nella Strategia per il mercato unico digitale in Europa, la Commissione era giunta addirittura a sostenere che sarebbe dovuto riconoscersi all'interessato il diritto di decidere se pagare mediante valuta ordinaria o cedendo in propri dati personali, sostenendo che in questo modo gli sarebbe stato attribuito controllo pieno su di essi. Questa previsione, che non è poi confluita nel testo definitivo, risulta ancora

[142] GDPR, art. 5, comma 1, lett. a).
[143] GDPR, art. 6, comma 1, lett. a).
[144] EDPB, "Guidelines 05/2020 on consent under Regulation (EU) 2016/679", accessibile da https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, 7.
[145] Mantelero, Vaciago (n. 137), 565.
[146] EDPB, "Guidelines 05/2020 on consent under Regulation (EU) 2016/679", (n. 144), 7.
[147] Parlamento Europeo e Consiglio, Direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, Direttiva (UE) 2019/770, L 136/1 https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019L0770&from=DE.

più controversa alla luce delle ulteriori considerazioni elaborate dall'EDPB sul libero consenso, ed in particolare sull'elemento della cosiddetta condizionalità, con la quale ci si riferisce al fatto che la cessione dei dati non debba essere in alcun modo legata all'accettazione di condizioni contrattuali che non siano necessarie ai fini dell'esecuzione del contratto e del servizio. Si legge che il GDPR mira a garantire che "il trattamento dei dati per il quale è ricercato il consenso non diventi, direttamente o indirettamente, la controprestazione del contratto" [148]. E' difficile dunque immaginare in che modo la proposta della Commissione potrà trovare una concreta collocazione.

Ulteriori problemi sono posti dal terzo degli elementi richiamati, ossia la granularità[149]. Nel caso in cui i dati debbano essere trattati per fini molteplici, il soggetto dovrà fornire il proprio consenso separatamente per ciascuno di essi. Questo aspetto è strettamente correlato anche alla necessità che il consenso sia specifico. Tuttavia, come sopra accennato, l'utilizzo di algoritmi nelle tecniche di *data analysis* accresce il rischio che i dati siano trattati per fini diversi e ulteriori rispetto a quelli per i quali i dati erano stati originariamente raccolti. Si è anche fatto presente che in molti casi gli stessi sviluppatori degli algoritmi non sono in grado di prevedere con certezza in che modo i dati saranno trattati. Come può allora garantirsi che il soggetto interessato abbia a disposizione tutte le informazioni rilevanti e necessarie per prestare il proprio consenso al trattamento dei dati personali? Anche in questo caso, sorgono non pochi dubbi sull'effettivo rispetto della disciplina del GDPR. Questo prevede che l'utilizzo dei dati per fini secondari è ammissibile solo nella misura in cui il fine ulteriore sia compatibile con quello primario e sia necessario per l'esecuzione del contratto[150].

A tal proposito, tuttavia, è stata sollevata un'obiezione relativa all'ipotesi in cui i dati siano utilizzati come vera e propria controprestazione, dal momento che in tal caso, quantomeno in termini economici, lo scopo del contratto consiste proprio nella cessione dei dati al fine di accedere al servizio. Si potrebbe dunque sostenere che in questo caso il trattamento dei dati sia contrattualmente necessario, poiché costituisce il mezzo di pagamento. È più ragionevole, tuttavia, immaginare che la CGUE prediligerà un'interpretazione più restrittiva della nozione, coerente con i dubbi qui esternati di compatibilità con la disciplina vigente[151].

Ultima condizione perché il consenso sia libero, è che questo possa essere rifiutato o ritirato senza che ciò comporti alcun detrimento, costo o svantaggio a scapito dell'interessato[152].

---

[148] EDPB, "Guidelines 05/2020 on consent under Regulation (EU) 2016/679", (n 144), 10.
[149] Ibid, 12.
[150] Prof. Dr. Mitrou, (n. 131), 48.
[151] Philipp Hacker, "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things", (2017), vol. 7 no. 4 *International Data Privacy Law*, 266-286, accessibile da https://academic.oup.com/idpl/article/7/4/266/4102081.
[152] EDPB, "Guidelines 05/2020 on consent under Regulation (EU) 2016/679", (n. 144), 13.

Gli altri due requisiti richiesti dal GDPR affinché il consenso sia valido, ossia la specificità e l'informazione, sono strettamente correlati e complementari al primo. Da un lato, infatti, la prima condivide molti profili con la granularità, mentre dall'altro va da sé che il consenso sia libero solo nella misura in cui l'interessato sia adeguatamente informato, abbia piena contezza di chi sia il titolare del trattamento, di quali tipologie di dati saranno raccolte e per quali fini saranno utilizzati, dell'esistenza del diritto di ritirare il consenso, delle informazioni sul trattamento automatizzato dei dati, ai sensi dell'art. 22 GDPR e, infine, dei possibili rischi legati al trasferimento dei dati verso Paesi terzi[153].

I problemi legati al consenso come base giuridica valida hanno portato a ricercare basi diverse che potessero giustificare e legittimare il trattamento dei dati. Si è fatto ricorso in particolare al legittimo interesse[154] (del titolare del trattamento o di un terzo) che, a norma dell'art. 6, deve comunque essere bilanciato rispetto ai diritti del soggetto interessato. Ai sensi della disposizione in esame, il trattamento dovrà essere necessario al soddisfacimento del suddetto interesse, risultando dunque insufficiente un collegamento soltanto potenziale[155]. Né si potrà ricorrere a questa base giuridica nel caso in cui esistano soluzioni alternative e meno lesive in termini di tutela dei dati personali che ne garantiscano il soddisfacimento. Dal momento che la base giuridica che legittima il trattamento dei dati deve essere individuata e comunicata prima che questo abbia inizio, non sarebbe possibile per il titolare, nel caso in cui ad esempio il soggetto ritiri il proprio consenso, proseguire il trattamento facendo deliberatamente ricorso ad una base giuridica diversa[156].

Il principio di trasparenza e il diritto d'informazione

Congiuntamente alla liceità, l'art. 5 fa riferimento anche alla correttezza e alla trasparenza[157]. Con riguardo a quest'ultimo profilo si è già fatta menzione dei problemi posti soprattutto dall'impiego di algoritmi *machine learning*, il cui funzionamento e i cui risultati sono spesso imprevedibili per gli stessi sviluppatori.

Occorre sottolineare che assicurare piena trasparenza, ponendo i soggetti interessati nelle condizioni di comprendere effettivamente come vengono trattati, analizzati ed elaborati i loro dati, aumenta il grado di fiducia di questi ultimi, incoraggiando lo sviluppo di nuove tecnologie.

Il principio in esame è inoltre strettamente correlato al diritto di informazione di cui gode l'interessato ai sensi dell'art. 13 GDPR. Nello specifico quest'ultimo avrà diritto, prima che il trattamento abbia inizio, a conoscere l'identità e i contatti del titolare del trattamento e del responsabile (laddove sia stato

[153] Ibid, 15.
[154] GDPR, art. 6 lett. f).
[155] Prof. Dr. Mitrou, (n. 131), 41.
[156] EDPB, "Guidelines 05/2020 on consent under Regulation (EU) 2016/679", (n. 144), 25.
[157] GDPR, art. 5 lett. a).

nominato), le finalità e la base giuridica, gli eventuali terzi destinatari dei dati e l'intenzione del titolare di trasferire i dati verso Paesi terzi. In aggiunta, il titolare avrà l'obbligo di informare l'interessato di tutti i diritti di cui gode, fra cui il diritto di ricevere adeguate informazioni nel caso in cui il trattamento preveda decisioni automatizzate, inclusa la profilazione[158].

Uno degli aspetti più problematici resta quello concernente le informazioni correlate all'assunzione di decisioni automatiche. La norma in esame riconosce infatti all'interessato il diritto di ricevere tutte le informazioni adeguate circa la logica sottostante la decisione assunta. L'Art. 29 WP ha emanato delle linee-guida sul punto[159], specificando che non è necessario fornire all'interessato una spiegazione dettagliata del complesso funzionamento dell'algoritmo, né tantomeno i dettagli riferiti ad una decisione nello specifico ma, perché gli obblighi di cui all'art. 22 siano adeguatamente adempiuti, sarà sufficiente che questo riceva una spiegazione generale sul meccanismo impiegato, purché alla luce di tale spiegazione sia in grado di comprendere le ragioni che sostengono la decisione assunta. Considerazione che mostra la sua contraddittorietà soprattutto se analizzata alla luce del successivo art. 14 e dell'interpretazione datane dalle suddette linee-guida.

L'articolo attribuisce all'interessato il diritto di ottenere, una volta che il trattamento sia iniziato, ulteriori informazioni riguardo la logica che sottende al trattamento e le conseguenze di quest'ultimo. Nonostante il tenore letterale della norma possa far ritenere il contrario, è stato infatti evidenziato che la disposizione non attribuisce all'interessato alcun diritto a ricevere informazioni diverse e ulteriori rispetto a quelle dovute ai sensi dell'art. 13, differendo le due norme solo per il momento in cui l'informazione viene fornita, che sarà nel primo caso prima che il trattamento abbia inizio, nel secondo invece una volta che questo sia già stato intrapreso. L'interessato avrà comunque diritto ad ottenere soltanto una spiegazione generica. Fra le buone pratiche suggerite dalle linee-guida, l'Art. 29 WP include anche quella di fornire una spiegazione in termini più ampi del modo in cui gli algoritmi funzionano e analizzano i dati nell'ipotesi in cui ciò possa essere utile agli esperti per valutare se il processo di decisione automatizzata funzioni o meno. Tale indicazione lascia tuttavia un margine d'incertezza, poiché non viene chiaramente definito in quali casi le ulteriori informazioni siano obbligatoriamente dovute o meno[160].

Il discorso si complica ancor di più se si tiene conto di altri due elementi[161]. Da un lato, dal momento che la *ratio* della norma è quella di consentire all'interessato di comprendere pienamente come vengono assunte le decisioni che lo riguardano e quali effetti ne conseguono, non soltanto le informazioni gli dovranno essere fornite - come d'altronde espressamente indicato dall'art. 12 - con un linguaggio

[158] GDPR, art. 22; FRA, ECHR, CoE, (n. 135), 99.
[159] Art. 29 WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", 25.
[160] Michael Veale e Lilian Edwards, "Clarity, Surprises, and further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, 400, accessibile da https://www.sciencedirect.com/science/article/pii/S026736491730376X?via%3Dihub,.
[161] Prof. Dr. Mitrou, Lilian, (n. 131), 56.

semplice e chiaro, ma inoltre la rilevanza delle informazioni da comunicare dovrebbe essere valutata dal punto di vista dell'interessato, ossia di un soggetto che nella maggior parte dei casi possiede una conoscenza minima, se non addirittura nulla, del meccanismo di funzionamento degli algoritmi. Ne consegue che anche le informazioni più basilari assumerebbero rilevanza. Dall'altro lato, come già evidenziato, le correlazioni trovate dagli algoritmi, sulla base dei quali vengono elaborati gli *output* finali, rimangono spesso oscure agli stessi programmatori e anche qualora non lo fossero, sarebbero comunque difficili da esprimere con un linguaggio umano. La disposizione è poi carente anche nella parte in cui non prevede che debbano essere fornite informazioni sulle modalità impiegate per "addestrare" gli algoritmi[162]. Questa rappresenta infatti una fase cruciale per determinare quale sarà l'esito della decisione, nonché il suo impatto sull'individuo, pertanto l'assoluta trasparenza sotto questo profilo è indispensabile al fine di valutare concretamente la correttezza e la sostenibilità della decisione sia in termini etici che giuridici.

In merito al rapporto fra diritto all'informazione, utilizzo degli algoritmi e validità del consenso, si è peraltro espressa di recente la Suprema Corte di Cassazione[163], con una massima di grande rilevanza. La Corte ha infatti affermato che "il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati". La Corte, ribaltando la conclusione del Tribunale nel grado di appello, ha dunque accolto l'indirizzo più restrittivo, in virtù del quale viene riconosciuto all'interessato il diritto a ricevere informazioni specifiche sul funzionamento dell'algoritmo posto alla base del trattamento dei dati personali.

I principi di correttezza ed esattezza

Il principio di correttezza[164], invece, va inteso in termini più ampi. Questo attiene al rapporto fra titolare del trattamento e soggetto interessato ma, soprattutto, al modo in cui i dati vengono trattati. Quando il trattamento coinvolge l'impiego di sistemi AI, tale principio ne impone un utilizzo etico[165]. Un errore dell'algoritmo, infatti, potrebbe tradursi in una forma di discriminazione dell'interessato, in un pregiudizio o in un vero e proprio danno. Per evitare che ciò accada, bisogna intervenire già nella fase

[162] Veale, Edwards, (n. 160), 400.
[163] Cassazione civile sez. I, 25/05/2021, n.14381.
[164] GDPR, art. 5, lett. a).
[165] Prof. Dr. Mitrou, (n. 131), 43-46; vedi diffusamente Gruppo di esperti del MISE sull'Intelligenza Artificiale, (n. 122); High-level expert group on Artificial Intelligence set up by European Commission, *Ethics guidelines for trustworthy AI,* (2019). L'adozione un approccio etico ed antropocentrico nello sviluppo dell'AI è il cuore della Proposta Italiana per l'Intelligenza Artificiale, ispirata ai principi generali già elaborati a livello europeo. Il documento fa riferimento alle stesse preoccupazioni qui riferite, auspicando che l'Unione Europea sia in grado di adottare un approccio comune e rispettoso dei propri principi fondamentali, con riguardo a tutti i profili problematici derivanti dall'evoluzione delle nuove tecnologie. L'ottica dalla quale si guarda alla questione è sempre la stessa, cioè quella di garantire ad ogni costo il rispetto dell'uomo e della sua integrità.

di programmazione, prevenendo così risultati non voluti. Tuttavia, bisogna essere consapevoli del fatto che ogni algoritmo non rappresenta altro che il riflesso di standard e valori sociali, portando con sé i pregiudizi e condizionamenti che ne derivano.

È molto importante, dunque, che i dati trattati siano corretti, che siano sufficientemente rappresentativi della realtà, cercando di arginare quanto più possibile il rischio di risultati viziati. Rischi destinati ad essere ulteriormente enfatizzati dal continuo aggiornamento e dai continui "miglioramenti" che gli algoritmi stessi fanno della propria selezione. Sarebbe un errore, infatti, ritenere che gli algoritmi siano in grado di correggere i vizi in essi inglobati al momento della programmazione, poiché questi sono in grado di apportare cambiamenti intesi piuttosto come il perfezionamento dei risultati ottenuti sulla base di quanto imparato in precedenza. Continuando ad assumere come vere e corrette le informazioni originarie, non vi sarà dunque alcuna correzione del vizio iniziale ma, semmai, un suo aggravamento.

Alla luce di queste considerazioni si spiega la proposta avanzata dall'Information Commissioner's Office (da qui in poi "ICO") di adottare un approccio proattivo[166], volto ad anticipare l'intervento alla fase di elaborazione degli algoritmi e a coinvolgere nei processi di revisione anche altri soggetti, a cui spetterebbe il compito di valutare l'impatto etico e sociale che la loro implementazione potrebbe avere. In alternativa, si è proposto di testare gli algoritmi sulla base di alcuni parametri ritenuti particolarmente rilevanti. Questa soluzione implica tuttavia l'utilizzo di strumenti tecnici avanzati, nonché l'introduzione di nuove regole volte a disciplinare, come accade già in altri settori, un sistema di autorizzazioni. In altre parole, tali sistemi potrebbero entrare in commercio solo una volta che si sia accertato che non vi siano rischi per gli utenti[167].

Focalizzarsi su questo aspetto è ancora più importante se si considera che i sistemi AI vengono spesso impiegati per assumere decisioni che si presumono dotate di un maggior grado di oggettività rispetto a quelle che un essere umano sarebbe in grado di assumere. Da ciò deriva infatti che, facendo affidamento sui risultati prodotti dai sistemi AI, noi stessi ne subiamo l'influenza, modificando di conseguenza non soltanto il modo in cui vediamo il mondo, ma anche quello in cui lo regolamentiamo[168].

---

[166] Michael Butterworth, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, 264-265, accessibile da https://www.sciencedirect.com/science/article/pii/S026736491830044X?via%3Dihub.

[167] Si spinge in questo senso anche la risoluzione del Parlamento Europeo sulla responsabilità civile nei sistemi d'intelligenza artificiale, seguita dalla proposta di Regolamento presentata dalla Commissione. Il regime di responsabilità applicabile a ciascun sistema dovrebbe dipendere infatti da una previa valutazione del livello di rischio che questo presenta. I sistemi sarebbero dunque distinti in sistemi ad alto rischio oppure a rischio medio-basso, e mentre per i primi opererebbe un regime di responsabilità oggettiva, nel secondo caso troverebbe applicazione la semplice responsabilità per colpa. Il livello di rischio andrebbe comunque stabilito ex ante, cioè prima che il sistema entri in commercio. (Parlamento Europeo, *Regime di responsabilità civile per l'intelligenza artificiale*, Risoluzione del Parlamento europeo del 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale, 2020/2014; EC, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final).

[168] Prof. Dr. Mitrou, (n. 131), 45-46.

Da ultimo, è senz'altro rilevante che il principio di correttezza - e *latu sensu* di non discriminazione - trovi applicazione anche nell'ambito del diritto alla concorrenza. L'esempio più evidente è quello della discriminazione sui prezzi, che i consumatori potrebbero subire proprio in ragione dei profili creati mediante algoritmi[169].

Il GDPR fa poi riferimento al principio di esattezza[170], richiedendo che vengano predisposte tutte le misure necessarie a garantire la tempestiva cancellazione o rettificazione dei dati inesatti rispetto alle finalità per cui sono stati raccolti. Ciò che s'intende preservare, dunque, è la qualità dei dati, valutata in relazione al contesto in cui avviene il trattamento[171]. Non è sufficiente, infatti, che la qualità e la correttezza dei dati siano valutate al momento della loro raccolta, ma è necessario che ne venga fatta un'adeguata valutazione anche nel corso delle fasi successive, e dunque per ciò che concerne sia la loro analisi che le decisioni basate su di essi.

L' ICO [172] ad esempio, sosteneva che un certo margine di "confusione" fosse tollerabile nel caso di analisi focalizzate esclusivamente su *trend* generali, mentre il trattamento i dati inesatti sarebbe certamente problematico se utilizzato per la profilazione di singoli individui. Ai programmatori spetterebbe il compito di "addestrare" gli algoritmi fornendo loro dati adeguatamente rappresentativi della realtà, così da scongiurare eventuali forme di discriminazione che potrebbero derivare dal far rispecchiare agli algoritmi pregiudizi tipicamente umani. È vero, come si è già evidenziato parlando dell'inadeguatezza del concetto di soggetto interessato come attualmente inteso dal GDPR, che il pregiudizio consistente in forme di discriminazione comporta primariamente un danno nei confronti di un gruppo e non di un singolo, ma altresì vero che vi sono delle circostanze in cui questa può tradursi in un danno individuale[173].

Si discute su quali siano i possibili rimedi che il singolo potrebbe utilizzare in queste ipotesi. Butterworth[174] esplora la possibilità di contestare che il trattamento sia legittimato da un'idonea base legale o di fare appello a quanto sancito dall'art. 22 relativamente alle decisioni automatizzate. L'autore, tuttavia, propende maggiormente per una terza via, ossia quella di riportare questo tipo di problemi al novero del principio di correttezza e non di quello di esattezza.

---

[169] EDPB, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, 8-10.
[170] GDPR, comma 1, lett. d).
[171] Prof. Dr. Mitrou, (n. 131), 51.
[172] ICO, "Big Data, artificial intelligence, machine learning and data protection", (2018), 43, accessibile da https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf,.
[173] A tal proposito può farsi l'esempio di alcuni algoritmi impiegati nella valutazione del rischio di recidiva nella commissione di determinati reati, destinati ad influenzare le decisioni assunte dai giudici nei confronti di individui accusati di determinati crimini. Se algoritmi di questo tipo decidessero sulla base di un pregiudizio, ad esempio nei confronti di uno specifico gruppo sociale o etnico, è chiaro che sarebbe il singolo individuo nei confronti del quale viene assunta la decisione a soffrire il danno.
[174] Butterworth, (n. 166), 260-261.

Al di là dell'inquadramento giuridico verso il quale si propende, il richiamo all'art. 22 parrebbe rilevare almeno sotto un altro punto di vista[175]. Si può parlare di rischi legati all'inesattezza dei dati, infatti, anche in termini di errata interpretazione dei risultati prodotti dagli algoritmi. In molti casi le correlazioni fra i dati trovate da questi ultimi non sono immediatamente comprensibili dall'uomo, né viene fornita un'adeguata spiegazione dei meccanismi ad esse sottese. Ne consegue non soltanto un elevato rischio che il loro effettivo significato sia frainteso, ma anche che sia appunto difficile, se non impossibile, garantire il diritto di ricevere adeguate informazioni nel caso in cui vengano assunte decisioni automatizzate.

I principi di limitazione delle finalità, di minimizzazione dei dati e di limitazione alla conservazione dei dati

Un altro principio a cui, seppure indirettamente, si è già fatto riferimento, è quello di limitazione delle finalità[176], in virtù del quale i dati dovranno essere trattati per finalità specifiche e legittime, comunicate al soggetto interessato prima che il trattamento stesso abbia inizio, attribuendogli così pieno controllo sui propri dati personali e consentendo di determinare con certezza se vi è pieno rispetto della disciplina. Il trattamento per finalità ulteriori potrà avvenire solo nelle limitate ipotesi in cui queste siano compatibili con la finalità principale o se a fini statistici e di ricerca. Facendo riferimento all'utilizzo degli algoritmi *machine learning*, che si basano proprio sull'analisi sempre più scrupolosa di dati, al fine di trarne ulteriori informazioni e accrescerne il valore, è chiaro che il trattamento a cui i dati saranno effettivamente sottoposti e il fine per cui questo avverrà divengono dunque non soltanto imprevedibili, ma anche non voluti dal responsabile/programmatore.

Il principio di minimizzazione[177], in virtù del quale i dati raccolti dovranno essere adeguati, pertinenti e necessari alla luce delle finalità perseguite, costituisce l'estrinsecazione e la specificazione del più generale principio di proporzionalità già sancito dal legislatore europeo con la Direttiva 95/46/EC. Il responsabile del trattamento sarà dunque chiamato al duplice e difficile compito di individuare non soltanto le finalità precise per cui i dati devono essere trattati, ma anche quali dati siano in tal senso rilevanti, operando un difficile bilanciamento fra gli interessi che si contrappongono.

La lett. e) dell'art. 5 del GDPR fa poi riferimento al principio di limitazione alla conservazione dei dati, in virtù del quale questi non possono essere conservati per un arco di tempo superiore a quello necessario per il conseguimento delle finalità per cui sono trattati, ad eccezione dei casi in cui vi siano ragioni di pubblico interesse o il trattamento sia effettuato a fini statistici o di ricerca. In merito a questo principio

[175] Prof. Dr. Mitrou, (n. 131), 52.
[176] GDPR, art. 5, comma 1, lett. b).
[177] GDPR, art. 5, comma 1, lett. c).

valgono in parte le medesime considerazioni fatte per quanto riguarda il principio di minimizzazione. Il valore dei dati, infatti, cresce proporzionalmente alla possibilità di correlarli fra loro e trarne quante più informazioni possibili. Limitare il periodo di conservazione dei dati si traduce in un limite al loro valore. In un certo senso si potrebbe ritenere (e vi è chi sostiene[178]) che attraverso le eccezioni summenzionate il GDPR abbia aperto uno spiraglio allo sfruttamento dei dati per un periodo ulteriore rispetto a quello necessario per il conseguimento della finalità principale, ma non si possono trascurare le considerazioni già fatte sulla difficoltà di tracciare con certezza un confine fra utilizzo a fini statistici e di ricerca e utilizzo di dati per fini diversi. È interessante notare comunque che venga lasciata agli Stati Membri una certa discrezionalità nel determinare quali siano le misure adeguate a garantire il rispetto dei diritti fondamentali dell'interessato e che consentirebbero dunque il trattamento dei dati.

Il principio di sicurezza

Il penultimo dei principi elencati dall'art. 5 è quello di sicurezza[179], con il quale si auspica l'adozione di tutte le misure tecniche ed organizzative adeguate a garantire la tutela dei dati da trattamenti non autorizzati o illeciti o dalla loro perdita, distruzione o danni accidentali. A questo fa eco l'art. 32 del GDPR, che pone proprio in capo al titolare e al responsabile del trattamento l'obbligo di individuare e porre in essere le misure necessarie alla sicurezza, tenendo conto anche dello stato di avanzamento delle tecnologie.

Sotto questo profilo deve evidenziarsi che l'UE ha fatto notevoli passi avanti, ponendo un'attenzione particolare al tema della *cybersecurity*. Come si è già anticipato, con il Cybersecurity Act entrato in vigore nel giugno del 2019, si è inteso infatti alzare gli standard di sicurezza dei sistemi informatici all'interno degli Stati membri, favorendo la cooperazione e la condivisione delle migliori tecniche al momento esistenti.

Il principio di responsabilità, il Data Protection Impact Assessment e i Codici di condotta

Da ultimo, il comma 2 l'art. 5 fa menzione del principio di responsabilità. Nonostante sia posto in chiusura, tale principio costituisce il principio-quadro entro il quale si muovono tutti gli altri previamente elencati[180]. E' proprio questa seconda parte della disposizione, infatti, che individua il titolare del

[178]Mayer-Schonberger, Padova, (n. 14), 331.
[179] GDPR, art. 5, comma 1, lett. f).
[180] È doveroso, al fine di comprendere pienamente il contenuto sostanziale del principio di responsabilità, fare una premessa di natura terminologica sulla differenza esistente fra la versione in lingua italiana e quella in lingua inglese del GDPR. Nella versione inglese, infatti, ci si riferisce al principio di responsabilità nel senso qui inteso con il termine *accountability*, volto ad indicare l'obbligo di garantire il rispetto di disposizioni poste in essere indipendentemente dalla volontà del soggetto che è tenuto a farle rispettare. Concetto da tenere distinto sia rispetto a quello di *responsability* che a quello di *liability*, che pure nella versione italiana

trattamento come il soggetto che in concreto ha il dovere di garantire il rispetto dei suddetti princìpi, gravando su di lui anche l'obbligo di dare la prova di essere effettivamente in grado di farlo[181]. Ciò si traduce nell'obbligo di fornire spiegazioni ragionate e adeguate del perché sono state adottate determinate misure piuttosto che altre, anche sulla base dei risultati delle analisi preventive condotte tenuto conto delle circostanze e delle finalità del trattamento.

Non si può negare l'enorme difficoltà di fronte alla quale si trovano i titolari del trattamento nel cercare di adempiere correttamente a tali obblighi nel contesto delle nuove tecnologie. La naturale opacità dei sistemi AI, da cui consegue che sia quasi impossibile prevedere o spiegare gli effettivi risultati del trattamento, si traduce inevitabilmente in un ostacolo al compimento di una preventiva e certa valutazione del livello di rischio a cui sarebbero esposti i dati personali[182]. Il titolare dovrebbe essere in grado di dimostrare non solo che gli algoritmi stanno lavorando esattamente secondo le istruzioni che sono state impartite loro, ma anche che i risultati da essi prodotti non siano in alcun modo discriminatori, errati o pregiudizievoli.

Gli strumenti di cui generalmente il titolare del trattamento si avvale al fine di adempiere ai suddetti obblighi sono essenzialmente il Data Protection Impact Assessment[183] (da qui in poi "DPIA") e i codici di condotta[184].

Ai sensi dell'art. 35 GDPR, la DPIA dovrà obbligatoriamente essere disposta per i trattamenti "ad alto rischio". Il *considerando 75* del GDPR aiuta a definire tale concetto, includendovi i trattamenti potenzialmente discriminatori, o che possono determinare un furto di identità, un danno economico o alla reputazione, la privazione della libertà personale o del controllo sui propri dati personali, la violazione di dati sensibili dell'interessato e via discorrendo. L'art. 35 individua le ipotesi che con assoluta certezza ricadono nella definizione di alto rischio, fra le quali ve ne sono alcune certamente rilevanti nel contesto delle nuove tecnologie, tanto che si è giunti addirittura ad ipotizzarne l'obbligatorietà ogni qualvolta sia previsto l'impiego di sistemi AI, laddove questo implichi il trattamento di dati personali[185]. Per quanto condivisibile, tale osservazione risulta incompleta. Come osservato, infatti, il trattamento mediante algoritmi pone un serio problema di distinzione fra dati

---

vengono tradotti con il termine "responsabilità". Nel primo caso, infatti, il riferimento è alla capacità di autodeterminazione della parte, mentre il secondo termine indica il concetto nostrano di responsabilità civile. (Nicola Fabiano, "GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali fra etica e cybersecurity", 2019, (Go Ware) 8, accessibile da https://www.perlego.com/book/1078890/gdpr-privacy-consapevolezza-e-opportunit-analisi-ragionata-della-protezione-dei-dati-personali-tra-etica-e-cybersecurity-prefazione-di-giovanni-buttarelli-pdf).

[181] FRA, ECHR, CoE, (n. 135), 101-103.

[182] Prof. Dr. Mitrou, (n. 131), 60-61.

[183] GDPR, art. 35. E' uno degli strumenti innovativi introdotti dal GDPR, coerente con il generale principio di *risk-assessment*. Consiste in una valutazione preventiva che, tenuto conto del tipo di trattamento, della natura dei dati e delle finalità perseguite, consente di individuare il livello di rischio per i dati personali e l'adeguatezza delle misure tecniche ed organizzative adottate dal titolare del trattamento al fine di ridurlo.

[184] GDPR, art. 40.

[185] Prof. Dr. Mitrou, (n. 131), 65.

personali e non e nulla esclude che dal trattamento di dati non personali se ne possano invece ricavare altri che consentono l'identificazione di un individuo preciso. Sarebbe forse dunque più corretto disporre l'obbligatorietà della DPIA ogni qualvolta si debba procedere al trattamento di dati utilizzando nuove tecnologie, estendendo la tutela del GDPR oltre i confini attualmente esistenti per scongiurare concretamente il rischio di violazioni sui dati personali.

Un altro strumento utile contemplato dal GDPR come mezzo per prevenire i rischi di violazione dei dati personali è costituito dai codici di condotta. Si tratta di strumenti di autoregolamentazione che le associazioni o gli altri organismi rappresentanti i titolari o responsabili del trattamento possono elaborare, modificare o prorogare al fine di migliorare l'applicazione del GDPR avendo riguardo delle caratteristiche specifiche dei vari settori e delle esigenze proprie delle micro, piccole e medie imprese. La loro adozione non è obbligatoria, ma fortemente incoraggiata dagli Stati Membri, le autorità di controllo e la Commissione, in quanto si tratta di strumenti che favoriscono le imprese nel condurre la propria attività nel pieno rispetto della disciplina prevista dal GDPR[186].

Molti autori riconoscono la potenziale utilità di questi strumenti – sia la DPIA che i codici di condotta – nel contribuire alla risoluzione di alcuni dei problemi posti dai Big Data, con particolare riferimento ai pericoli – di cui sopra si è detto – in cui l'individuo incorre non in quanto tale, ma in quanto membro di un determinato gruppo. Si mette in luce, infatti, che un'analisi preventiva del rischio potrebbe avere ad oggetto non soltanto i rischi strettamente legati alla tutela dei dati personali ma, più in generale, i pericoli per la salvaguardia dei diritti fondamentali[187].

La potenziale utilità di questi strumenti non deve però far dimenticare la difficoltà del loro concreto utilizzo in contesti innovativi come quelli che si stanno qui esaminando[188]. Anzitutto l'esperienza insegna che nell'evoluzione tecnologica non è sempre chiaro sin dal primo momento in che modo una specifica tecnologia sarà effettivamente utilizzata e, soprattutto, quali conseguenze possono derivare dal suo utilizzo, pertanto ogni valutazione d'impatto preventiva, basata sull'impiego attuale o potenziale della tecnologia, potrebbe non essere sufficiente a prevedere i rischi effettivamente correlati al suo utilizzo. Il lasso di tempo che normalmente intercorre dal momento in cui una nuova tecnologia viene

---

[186] Laurens Naudts, "How machine learning generates unfair inequalities and how data protection instruments may help in mitigating them", in Leenes, Ronald, Rosamunde van Brakel, Serge Gutwirth, and Paul de Hert *Data Protection and Privacy: The Internet of Bodies* (London: Bloomsbury Publishing Plc, 2018), para 3.1 (b), accessibile da https://www.perlego.com/book/875482/data-protection-and-privacy-the-internet-of-bodies-pdf.

[187] Ibid, para 2.1. L'opinione è condivisa anche dal gruppo di esperti incaricato dal MISE di elaborare delle proposte per una strategia italiana sull'AI che, condividendo la necessità di monitorare l'utilizzo delle nuove tecnologie e riconoscendo l'efficacia dell'approccio adottato in materia di dati personali, auspica l'introduzione di un nuovo strumento pensato ad hoc per il contesto AI e costruito sulla falsariga della DPIA. Lo strumento prenderebbe il nome di *Trustworthy AI Impact Assessment* (TAIA), che mette in chiaro lo scopo ultimo al quale questo tende: assicurare che la nuova tecnologia venga utilizzata nel pieno rispetto dei canoni etici e dei principi fondamentali del nostro ordinamento. Tale strumento dovrebbe consentire di tenere conto anche della qualità, dell'aggiornamento e della varietà dei dati utilizzati, includendo anche le procedure di *Human Rights Impact Assessment* (HRIA) elaborate dal Consiglio d'Europa.

[188] Prof. Dr. Mitrou, (n. 131), 65-67.

introdotta sul mercato e quello in cui se ne può valutare l'impatto con piena cognizione di causa potrebbe tradursi in un danno notevole per la tutela dei dati personali e non solo.

L'ampliamento dell'ambito di indagine su cui verte la valutazione preventiva renderebbe poi doveroso un contestuale ampliamento del novero dei soggetti in essa coinvolti. La disciplina attuale, pur facendo gravare l'onere di disporre la DPIA sul titolare del trattamento e, laddove presente, sul responsabile, prevede già la possibilità che vengano coinvolti e ascoltati il soggetto interessato (personalmente o per il tramite di un ente che lo rappresenti) e degli *stakeholders*, al fine di porre l'attenzione su aspetti che altrimenti rischierebbero di essere trascurati. Se l'obiettivo da raggiungere si amplia fino ad includere una protezione complessiva dei diritti fondamentali potenzialmente messi a rischio dal trattamento dei dati, è ragionevole ritenere che dovranno essere coinvolti soggetti con un *background* di conoscenze più ampio.

Diritto di accesso

Si è già più volte fatto riferimento al diritto di accesso sancito dall'art. 15 del GDPR. Ai sensi di tale disposizione l'interessato avrà diritto non soltanto a sapere se i propri dati personali siano o meno soggetti a trattamento, ma anche ad ottenere informazioni specifiche con riferimento a determinati elementi (categorie di dati trattati, finalità, soggetti ai quali i dati vengono trasferiti, periodo di conservazione dei dati, diritti esercitabili dall'interessato). L'esercizio di tale diritto va comunque bilanciato rispetto ai diritti degli altri soggetti coinvolti, con la conseguenza che l'accesso ai dati da parte dell'interessato non dovrà violare i diritti di proprietà industriale e gli interessi economici del titolare. L'interessato potrà pertanto chiedere l'accesso ad informazioni precise e, dal canto suo, il titolare sarà tenuto a porre in essere tutte le misure tecniche ed organizzative utili e ragionevoli al fine di garantirne il pieno esercizio.

L'esperienza maturata nel settore dei social media e dei motori di ricerca ha messo in luce che in questi contesti l'esercizio di tale diritto si risolve nella mera possibilità per l'interessato di seguire modelli e procedure predeterminate dal titolare, spesso di difficile attuazione, che finiscono con l'inficiare l'effettività della disposizione in esame[189]. Considerazioni senz'altro valide anche in riferimento al diritto di rettificazione dei dati sancito dall'art. 18 del GDPR. Diritto che assume particolare rilevanza nel contesto della *big data analysis* in cui la correttezza delle informazioni "grezze" fornite ai sistemi è

[189] Pieremilio Sammarco, "Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato" in Tosi Emilio, Antonello Soro, Vincenzo Franceschelli, Giovanni Buttarelli, and Ettore Battelli *Privacy Digitale: Riservatezza e Protezione Dei Dati Personali Tra GDPR e Nuovo Codice Privacy*, (Vol. 21. Milano: Giuffrè Francis Lefebvre, 2019), 165.

elemento imprescindibile perché il trattamento sia lecito e non si traduca in una sostanziale violazione dei diritti fondamentali.

Diritto alla portabilità dei dati

Ai sensi dell'art. 20 del GDPR, l'interessato avrà diritto ad ottenere i propri dati in un formato leggibile e strutturato, nonché alla loro trasmissione ad un altro titolare del trattamento, anche direttamente se ciò è tecnicamente possibile, nell'ipotesi in cui i dati siano stati forniti sulla base del consenso o per l'esecuzione di un contratto o nel caso in cui il trattamento sia automatizzato. Nonostante i punti di contatto riscontrabili con il già menzionato diritto all'accesso, rileva che in tal caso il legislatore abbia disposto specifici presupposti e indicazioni relative al formato in cui i dati devono essere forniti all'interessato. I due diritti perseguono comunque fini diversi, dal momento che mentre il diritto all'accesso è funzionale alla concreta attuazione del principio di trasparenza, il diritto alla portabilità dei dati mira a favorire la libera circolazione dei dati, con la conseguenza che quest'ultimo avrà certamente un ambito di applicazione più ristretto del primo[190].

Tale diritto è stato ampiamente riconosciuto come uno dei più innovativi fra quelli introdotti dal GDPR in quanto, sebbene si tratti di un principio proprio della protezione dei dati personali, è destinato ad avere un impatto notevole sullo sviluppo delle tecnologie e sulla concorrenza. Assicurare il diritto alla portabilità dei dati presuppone l'utilizzo di strumenti e formati che ne consentano tecnicamente la trasmissibilità e assicura gli utenti dal rischio di soffrire le conseguenze negative dei cosiddetti "effetti *lock-in*"[191].

La norma, infatti, s'inserisce nel filone di disposizioni che mirano ad attribuire il totale controllo sui dati personali all'interessato, mirando a scongiurare ogni possibilità che questo si veda costretto a cedere i propri dati ad un determinato soggetto, senza avere poi potere di cambiare la propria scelta. Ne deriverebbe un intollerabile squilibrio di poteri a vantaggio del titolare, tanto nei confronti dell'interessato, quanto in quelli dei propri concorrenti. Già prima dell'entrata in vigore del GDPR era stato messo in luce che l'introduzione del diritto portabilità dei dati avrebbe avuto sia per le imprese/titolari che per i consumatori/interessati, favorendo un regime più trasparente e riducendo il rischio di pratiche scorrette o discriminatorie.

[190] Ettore Battelli, Guido D'Ippolito, "Il diritto alla portabilità dei dati" in Tosi, Emilio, Antonello Soro, Vincenzo Franceschelli, Giovanni Buttarelli e Ettore Battelli *Privacy Digitale: Riservatezza e Protezione Dei Dati Personali Tra GDPR e Nuovo Codice Privacy* (Vol. 21, Milano: Giuffrè Francis Lefebure, 2019), 190; Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, e Ignacio ca. "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services", (2018), vol. 34/no. 2 *The Computer Law and Security Report*, 194, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917303333?via%3Dihub.

[191] Battelli, D'Ippolito, (n. 190), 213.

La vocazione economica di questo diritto e gli effetti positivi sulla concorrenza che questo produce saranno tanto più evidenti e significativi proprio in relazione al contesto dei servizi e delle piattaforme digitali[192]. Il tenore letterale della norma, facendo esplicito riferimento al diritto dell'interessato di ottenere il trasferimento diretto dei dati da un titolare all'altro laddove ciò sia tecnicamente possibile è volta a favorire lo sviluppo di sistemi interoperabili e in grado di comunicare fra loro[193]. Proprio questo profilo fa sì che la norma trascenda i confini del diritto alla protezione dei dati personali, acquistando rilevanza anche in altri ambiti del diritto.

Diritto alla cancellazione dei dati

Certamente di grande rilevanza nel contesto dello sviluppo delle nuove tecnologie è il diritto alla cancellazione dei dati sancito dall'art. 17 del GDPR[194]. Si tratta di un diritto di origine giurisprudenziale, che ha trovato riconoscimento legislativo solo con l'entrata in vigore del GDPR, ponendosi sulla scia delle altre disposizioni finalizzate a garantire il pieno controllo sui dati da parte dell'interessato e rafforzare la tutela garantita a quest'ultimo[195].

Non si tratta però di un diritto assoluto. In primo luogo l'interessato avrà diritto di ottenere senza ingiustificato ritardo la cancellazione dei propri dati personali solo se le condizioni specificatamente elencate dal GDPR sono soddisfatte. Inoltre il diritto alla cancellazione dovrà essere bilanciato con gli altri diritti che vengono in rilievo, e specificatamente la libertà di espressione e il diritto d'informazione.

---

[192] Di questo aspetto ha dato conferma il fatto che la Commissione ne abbia fatto uso anche fra le più recenti proposte legislative in materia. Il Digital Market Act – di cui si dirà diffusamente più avanti - prevede infatti il riconoscimento del diritto alla portabilità dei dati anche agli utenti *"business"* che operano all'interno delle piattaforme digitali. Il fine è quello di indebolire la posizione dominante di cui godono tali piattaforme in virtù, fra le altre cose, proprio della grande disponibilità di dati su cui possono fare affidamento. Il tradizionale assunto che i dati siano beni non-rivali ed egualmente utilizzabili da tutti i concorrenti viene facilmente smentito se si fa riferimento ai dati prodotti dalle stesse piattaforme e conservati nei server di queste ultime, in quanto ne è precluso l'accesso a soggetti terzi. La nuova disciplina, invece, attribuisce ai *provider* più piccoli il diritto di trasferire i suddetti dati nei propri server ed utilizzarli. Si veda (Proposta della Commissione di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali COM(2020) 264 final). A dire il vero i primi commenti sulla normativa si sono dimostrati critici verso questa soluzione, mettendo in luce il fatto che decontestualizzare i dati implica una perdita di valore degli stessi, senza contare i problemi tecnici e di interoperabilità che potrebbero ostacolare l'effettivo esercizio di tale diritto. In alternativa è stato proposto di riconoscere il diritto di accesso diretto ai server delle piattaforme. (Si veda Joint Research Center (Commission), *The EU Digital Markets Act - A Report from a Panel of Economic Experts*, (2021) accessibile da https://publications.jrc.ec.europa.eu/repository/handle/JRC122910).

[193] De Hert, Papakonstantinou, Malgieri, Beslay, Sanchez. (n. 190), 197.

[194] Regolamento (UE) 679/2016 art. 17. *"L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1."*

[195] Sammarco, (n. 189), 168-171.

Il GDPR in realtà non determina in quali circostanze tali diritti debbano prevalere rispetto a quello di cancellazione dei dati, lasciando all'interprete l'arduo compito di svolgere una valutazione caso per caso, alla luce per principi di verità, completezza ed esattezza (con riferimento ai dati), nonché quelli di attualità, interesse collettivo e pertinenza dell'interesse perseguito. Nel celebre caso Manni[196] la CGUE ha affermato che finché sussiste un interesse pubblico alla fruibilità dei dati, l'interessato non potrà ottenerne la cancellazione.

Privacy-by-design e privacy-by-default

L'art. 25 del GDPR[197] pone in capo al titolare del trattamento l'ulteriore obbligo di predisporre, tenendo di tutte le circostanze concrete, tutte le misure tecniche ed organizzative adeguate volte ad attuare nella maniera più efficace i principi di protezione dei dati personali. Tale obbligo dovrà essere rispettato sia nella fase di scelta dei mezzi per il trattamento che nel momento in cui questo viene effettuato. Si tratta di un principio che assume particolare importanza soprattutto nei contesti più innovativi e nello sviluppo delle nuove tecnologie, poiché evidenzia la consapevolezza del legislatore europeo della necessità di intervenire sul piano tecnico prima che normativo al fine di garantire il pieno rispetto della disciplina sulla tutela dei dati.

In virtù di tale principio, infatti, è auspicabile che la tecnologia emergente sia in grado di "inglobare" i principi dettati dal GDPR, al punto che il rispetto di questi ultimi sia garantito dall'architettura stessa dei nuovi dispositivi e senza che ciò determini un peggioramento delle prestazioni. È incoraggiato dunque un atteggiamento proattivo e preventivo, piuttosto che reattivo e rimediale[198]. Lo scopo è quello di evitare che vi siano violazioni dei dati personali a scapito degli individui, intervenendo a monte del problema.

Questo approccio consente di conseguire anche un risultato ulteriore, ossia quello di conciliare al contempo la tutela dei dati alla sicurezza dei dispositivi. Verosimilmente, di fronte ai problemi sempre più rilevanti posti dallo sviluppo delle nuove tecnologie, tutto ciò sarà possibile grazie al loro utilizzo integrato, che consenta di ridurre i profili di rischio propri di ciascuna di esse e potenziarne le capacità. Uno degli esempi più interessanti in questo senso è rappresentato dalla possibilità di integrare i sistemi

[196] C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni,* [2015].
[197] Regolamento 679/2016, art. 25, comma 1, "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".
[198] Ann Cavoukian Ph.D, Information & Privacy Commissioner, Ontario, Canada, "Privacy by design - The 7 Foundational principles. Implementation and mapping of fair information practises", (2010), accessibile da https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

IoT con la tecnologia *blockchain* anche, ma non solo, tramite l'utilizzo degli *smart contract*[199]. Come si vedrà meglio nel prosieguo, questa soluzione potrebbe infatti migliorare i livelli di *compliance*, garantendo trasparenza e sicurezza nello scambio dei dati.

1.4.2 Le nuove proposte di regolamentazione

Intuendo la necessità di regolamentare ulteriormente il settore dei dati, soprattutto alla luce delle considerazioni concernenti la tutela della concorrenza a cui si è fatto in precedenza riferimento, la Commissione ha di recente elaborato ulteriori proposte legislative, che si collocano nell'ambito della European Data Strategy[200]. Con tale progetto l'UE aspira a porsi alla guida della rivoluzione digitale in atto, promuovendo la diffusione di regole compatibili con i principi fondanti dell'ordinamento europeo. I presupposti che hanno portato all'elaborazione di un progetto così ambizioso, che anticipa una stagione di riforme destinate ad avere un impatto certamente non limitato al solo profilo economico, sono molteplici. La Commissione[201] ha infatti messo in guardia sul fatto che bisogna intervenire adesso perché si possa garantire la sopravvivenza di un mercato pienamente concorrenziale nel corso dei prossimi anni e affinché l'UE possa aspirare ad avere un ruolo rilevante non solo a livello economico, ma anche politico, nel futuro prossimo.

D'altro canto, l'intervento auspicato dall'UE deve tenere conto anche degli altri attori che si muovono sul piano internazionale, ed in particolare USA e Cina che nello sviluppo di progetti per la raccolta e la gestione dei dati hanno adottato approcci diametralmente opposti fra loro ma comunque lontani dai princìpi cardine dell'UE. Anche per effetto della dottrina neo-liberale che ha dominato per lungo tempo, gli Stati Uniti tendono infatti ad affidare la raccolta dei dati soprattutto al settore privato, con elevati rischi di concentrazioni. Il modello cinese, al contrario, vede la forte presenza del controllo statale, senza garantire sufficientemente la tutela degli individui. L'UE ha grande interesse nel contribuire allo sviluppo di standard internazionali e nel guidare la creazione di modelli coerenti con i princìpi europei, così da consentire alle proprie imprese di mantenere una posizione competitiva nel contesto internazionale.

La Commissione ha più volte enfatizzato, infatti, che anche il trasferimento dei dati verso Paesi terzi debba avvenire in modo sicuro e rispettoso della legislazione europea, in una visione coerente anche con la giurisprudenza più recente della CGUE in materia di dati personali (sentenze Schrems I[202] e II[203])[204].

---

[199] Si tratta dei cosiddetti "contratti automatizzati". Per una trattazione diffusa si veda Capitolo II, paragrafo 2.3.
[200] Commissione, Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, *A European Data Strategy,* COM(2020) 66 final.
[201] Ibid.
[202] Caso C-362/14 *Maximillian Schrems c. Data Protection Commissioner* [2015].
[203] Caso C-311/18 *Data Protection Commissioner c. Facebook Ireland and Maximillian Schrems* [2020].
[204] Commissione, (n. 191), 23.

D'altronde Bruxelles è sempre stata considerata "la capitale del mondo" per l'antitrust, anche in virtù del fatto che le autorità competenti, sia nazionali che europee, hanno autonomo potere di iniziativa e d'intervento, a differenza di quanto avviene ad esempio per le omonime americane[205]. Negli Stati Uniti, infatti, il diritto antitrust viene applicato solo di fronte alle corti giudiziali e soltanto le corti federali hanno il potere di applicare la legge federale. Queste premesse lasciano dunque ben sperare per il successo delle iniziative europee a livello internazionale, ma va anche detto che l'influenza che l'UE sarà effettivamente in grado di esercitare sullo sviluppo di altre legislazioni dipende molto dal valore del mercato europeo.

Queste riflessioni hanno condotto, come sopra anticipato, all'elaborazione di diverse proposte legislative. Le più rilevanti, presentate dalla Commissione il 15 dicembre 2020 e ancora in attesa di superare l'ordinario iter legislativo, sono tre: il Data Governance Act[206], il Digital Service Act e il Digital Market Act. Questi ultimi compongono insieme il Digital Market Package[207]. Tutte le proposte rivestono la forma del regolamento, rispecchiando la chiara intenzione del legislatore di promuovere uno sviluppo uniforme su tutto il territorio.

Il Data Governance Act fa riferimento alla categoria dei cosiddetti *open data*, ossia i dati creati dagli enti pubblici, e mira alla creazione di uno spazio unico di condivisione con soggetti privati all'interno del territorio europeo, che consenta alle imprese di trarre un vantaggio economico ed ai cittadini europei di fruire di servizi migliori[208]. La proposta prevede l'introduzione di nuove regole sia per la condivisione che per il riutilizzo dei dati prodotti, sottolineando che ciò debba avvenire nell'assoluto rispetto della disciplina sulla tutela dei dati e senza che comporti forme di discriminazione nei confronti dei cittadini. A tal proposito, sono previsti specifici meccanismi di notifica e di controllo nei confronti dei soggetti che condividono i dati, nonché la creazione di un Comitato europeo per la condivisione dei dati, che promuova le *best practises* fra gli Stati Membri.

Il Digital Service Act prevede nuovi obblighi specifici per le piattaforme che erogano servizi digitali[209], attribuendo loro maggiori responsabilità in ragione del ruolo, della grandezza e dell'impatto che hanno sull'ecosistema digitale[210]. In questo modo si vogliono favorire l'innovazione, la crescita e la

---

[205] "Big tech faces competition and privacy concerns in Brussels", (23 Marzo 2019), *The Economist,* accessibile da https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels.

[206] EC, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, COM (2020) 767 final 2020/0340 (COD), accessibile da https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act.

[207] EC, *The Digital Service Act package*, accessibile da https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

[208] Chiara Benvenuto, Pietro Maria Mascolo, "Data Governance Act," verso uno spazio comune europeo dei dati: scenari e conseguenze", (11 dicembre 2020), *Agenda Digitale*), accessibile da https://www.agendadigitale.eu/.

[209] EC, *The Digital Service Act: ensuring a safe and accountable online environment*, accessibile da https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

[210] Si distingue in particolare fra: servizi intermediari, servizi di hosting, piattaforme online e grandi piattaforme online (che raggiungano più del 10% dei 450 milioni di consumatori in Europa).

competitività, creando nuove opportunità soprattutto per le PMI e le *start-up*, tutelando i consumatori e garantendo il rispetto dei diritti fondamentali. Tali obblighi riguardano soprattutto la rimozione di contenuti illegali e la trasparenza sulle sponsorizzazioni e i rapporti con soggetti terzi. Viene inoltre introdotto l'obbligo di condividere i dati con le autorità impegnate nei procedimenti, di segnalare attività illegali e di garantire termini di servizio rispettosi della disciplina sui diritti fondamentali. In alcuni casi è sancito l'obbligo di notificare e fornire informazioni agli utenti. Tali disposizioni dovranno essere rispettate anche dai soggetti che offrono servizi nel territorio dell'UE, pur essendo stabiliti altrove.

Queste regole, in realtà, non rivoluzionano il quadro esistente, ma coincidono in gran parte con quanto già previsto dalle *policy* interne delle società. In questo modo, però, si garantirebbe l'adozione di un complesso di disposizioni certo ed uniforme su tutto il territorio dell'UE, elemento che rappresenta una novità non certo di trascurabile importanza[211].

Questa proposta è stata tuttavia oggetto di critiche, poiché ritenuta inadeguata a garantire un'effettiva tutela del mercato, dal momento che si limita ad introdurre obblighi nei confronti di soggetti che hanno già assunto una posizione rilevante, piuttosto che intervenire a monte prevenendo la creazione di situazioni rischiose[212].

A questa osservazione si può però facilmente controbattere tenendo conto del fatto che la proposta in esame sia stata elaborata congiuntamente al Digital Market Act che, invece, mira proprio a regolamentare l'attività dei cosiddetti *"gatekeeper"*[213], cioè le piattaforme che hanno una posizione economicamente forte sul mercato e la cui attività influenza notevolmente il mercato interno, in grado di porsi come intermediarie fra un alto numero di utenti e di imprese (più di 45 milioni di utenti finali e più di 10 milioni di utenti *business* attivi mensilmente) e che abbiano mantenuto tale posizione sul mercato per un lungo periodo, al fine di controllarne la crescita e scongiurare ogni forma di abuso. La nuova regolamentazione mira dunque a favorire le imprese più piccole, che dipendono dalle grandi piattaforme, garantendo loro un mercato più equo all'interno del quale operare, nonché promuovere la creazione di *start-up* innovative e tutelare i consumatori garantendo loro ampia e libera scelta sui prodotti, congiuntamente alla possibilità di passare da un *provider* all'altro senza subire alcun detrimento.

I *gatekeeper* potranno continuare ad operare insieme a soggetti terzi, dovranno condividere i propri dati, fornire tutte le informazioni rilevanti sulle sponsorizzazioni e consentire alle imprese di promuovere prodotti e concludere contratti anche al di fuori delle piattaforme. Sarà invece precluso loro favorire i

---

[211] "EU needs new teeth as watchdog of Big Tech", (USA, 16 dicembre 2020), *Financial Times,* accessibile da https://www.ft.com/content/6d4b9dbc-c795-427d-b43e-741a26511abb.

[212] Martin Sandbu "Regulation alone will not strengthen Europe's digital sector", (USA, 21 dicembre 2020), *Financial Times,* accessibile da https://www.ft.com/content/53458590-4a33-4f11-9e1d-6d9c0b8ea5c1.

[213] EC, *The Digital Markets Act: ensuring fair and open digital markets*, accessibile da https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

propri prodotti a scapito di quelli di terzi, limitare la possibilità dei consumatori di accedere ad offerte esterne alla piattaforma e impedire loro di disinstallare *software* o *app* preinstallate. Per garantire il rispetto delle nuove misure, vengono riconosciuti alla Commissione speciali poteri investigativi, nonché la possibilità di imporre obbligazioni ulteriori se necessario e, infine, di irrogare sanzioni. Le sanzioni previste per la violazione delle suddette norme variano dall'irrogazione di multe alle richieste di rimedi temporanei ma - come ultima *ratio* - non si esclude la possibilità di ordinare lo smembramento delle compagnie.

A febbraio 2021 la Commissione ha pubblicato un Report elaborato da un gruppo di economisti del *Joint Research Centre*[214] che ha formulato dei preliminari commenti sulla disciplina proposta dal Digital Market Act. Il panel di esperti ha mostrato apprezzamento verso la scelta di introdurre un meccanismo *ex ante*, che consenta di imporre obblighi alle imprese non appena si accerti che queste superino le soglie dimensionali rilevanti ai fini della qualificazione come *"gatekeeper"*, abbandonando la tradizionale procedura a tre fasi, secondo la quale era necessario dapprima definire il mercato rilevante, poi valutare la condotta tenuta e, infine, individuare i rimedi adeguati. Vengono condivise infatti le considerazioni relative alle difficoltà nell'individuare con certezza il mercato rilevante su cui operano le piattaforme, dal momento che queste sono contemporaneamente attive su più mercati, alla pari di quelle nell'individuare i concorrenti. Allo stesso tempo non sono però mancate le critiche e i suggerimenti per soluzioni alternative e/o complementari[215].

---

[214] Joint Research Centre, *"The EU Digital Markets Act - A Report from a Panel of Economic Experts"* (n. 192).

[215] In primo luogo non viene condivisa la distinzione fatta fra gli obblighi disciplinati dagli artt. 5 e 6. del Digital Market Act Stando alla lettera della proposta, infatti, questi ultimi sarebbero suscettibili di essere "ulteriormente specificati", lasciando aperto uno sconveniente margine d'incertezza. Nel Report viene dunque suggerito di distinguere le attività delle piattaforme dividendole fra una *"black"* e una *"grey list"*. La prima dovrebbe includere tutte le attività considerate comunque pericolose per la concorrenza, rispetto alle quali continuerebbe ad operare il meccanismo di applicazione automatica degli obblighi di cui sopra. Per le attività incluse nella *grey list*, invece, verrebbe riconosciuto alle imprese il diritto di fornire la prova che queste non abbiano effetti negativi sulla concorrenza. Queste sarebbero tenute a rispettare gli obblighi loro imposti fino a che tale prova non venga effettivamente fornita, così da non vanificare gli effetti delle nuove misure previste. Le attività di *"tying and bundling"*, alle quali vengono riconosciuti anche effetti positivi, troverebbero così collocazione nella *grey list*, mentre ogni forma di discriminazione dei prodotti di soggetti terzi sarebbe ricondotta alla *black list*. Per queste ipotesi viene addirittura suggerito di introdurre la possibilità di apporre un arbitro che abbia potere di imporre misure vincolanti durante la fase di accertamento delle violazioni, così da contenere gli effetti negativi, spesso irreversibili. Per quanto riguarda le sponsorizzazioni, proprio in ragione della centralità loro riconosciuta nell'ambito dei *business model* delle piattaforme, si ritiene che gli obblighi attualmente previsti, consistenti primariamente nel garantire piena trasparenza sui prezzi pagati dai *business users* e sui meccanismi di valutazione delle *performances*, sono forse insufficienti. Sembrerebbe più opportuno riconoscere piuttosto l'accesso ai dati grezzi, consentendo agli utenti di scegliere secondo quali criteri svolgere le valutazioni. Grande attenzione è rivolta, infine, alla condivisione dei dati, definiti come *asset* strategico e assolutamente peculiare nell'economia moderna. Attualmente la proposta impone da un lato il divieto di utilizzare i dati per ottenere un vantaggio competitivo, a meno che si tratti di dati pubblici e, dall'altro, prevede invece degli obblighi di condivisione dei dati, distinguendo a seconda che questa avvenga all'interno o all'esterno della piattaforma. Nel primo caso i *business users* avrebbero diritto alla portabilità dei dati, previo consenso degli utenti finali (diritto costruito sulla falsariga di quanto sancito dal GDPR a favore del soggetto interessato), e il diritto di accesso a tutti i dati, aggregati e non. Si osserva, tuttavia, che la portabilità dei dati porta con sé dei rischi di obsolescenza e perdita di valore degli stessi conseguente alla loro decontestualizzazione, motivo per cui parrebbe più opportuno consentire agli utenti *business* di accedere ai dati direttamente dai *server* delle piattaforme. In questo modo, peraltro, si realizzerebbe il vero obiettivo posto dietro l'obbligo di condivisione dei dati, ossia quello di garantire la competizione "a monte". Nel caso di condivisione all'esterno della piattaforma, invece, è molto interessante – specie alla luce della vicenda Facebook – osservare che viene sancito il divieto di combinare fra loro dati prodotti all'interno di piattaforme diverse (es. dati di Facebook e Instagram).

Si è detto prima che l'importanza della tutela dei dati in termini concorrenziali è dovuta soprattutto al fatto che consumatori sempre più consapevoli dei propri diritti, terranno in considerazione il livello di tutela garantito nel trattamento dei propri dati personali nella scelta sull'acquisto di beni o servizi. Si è detto anche che, come avvenuto con il GDPR, l'approccio europeo tende ad attribuire maggior controllo ai soggetti interessati sui propri dati personali. Tuttavia, anche nel report viene evidenziata l'incisività del cosiddetto "paradosso sulla privacy". Legando la tutela dei dati al diritto antitrust ed attribuendo maggiori poteri alle autorità competenti, è possibile ovviare alle conseguenze negative di tale problema. Anche da questo punto di vista, le novità proposte dalla Commissione sono rilevanti, soprattutto per i notevoli poteri investigativi e di intervento che vengono attribuiti alla Commissione.

Dal canto suo, anche il Regno Unito dopo l'uscita ufficiale dall'UE si sta muovendo verso l'introduzione di nuove regole in ambito concorrenziale[216]. L'approccio scelto, però, differisce profondamente da quello dell'UE, dal momento che piuttosto che introdurre un set di regole valide per tutti i soggetti che operano sul mercato, si è preferito adottare nuovi codici di condotta che impongano obblighi specifici per le singole società, ad esempio Facebook e Google. Le autorità inglesi saranno chiamate a svolgere una valutazione caso per caso, al fine di qualificare o meno come "strategica" una società ed imporle di conseguenza delle regole da osservare. La scelta è dovuta alla considerazione che nel mercato digitale anche piccole acquisizioni possono comportare gravi distorsioni della concorrenza, e un'analisi concreta svolta tenendo conto delle peculiarità del singolo caso consentirebbe interventi mirati ed efficaci.

Parallelamente, si sta lavorando anche alla ricerca di soluzioni tecniche coerenti con il principio di maggior controllo sui dati da parte dei soggetti interessati, che potrebbero derivare dall'integrazione di tecnologie diverse fra loro, come *blockchain*, IoT e sistemi AI.

Sarebbe infatti scorretto ritenere che la sola regolamentazione sia sufficiente a garantire uno sviluppo sostenibile della tecnologia, dovendosi questa necessariamente accompagnare all'elaborazione di soluzioni di natura tecnica. Così come sarebbe scorretto ignorare che l'interdipendenza fra le varie tecnologie, la cui diffusione futura è destinata ad influenzarsi reciprocamente dal momento che proprio integrando le une con le altre è possibile massimizzarne le prestazioni[217].

L'ENISA ha individuato proprio la tecnologia *blockchain* come uno degli strumenti che potrebbe contribuire a rafforzare i livelli di sicurezza nella trasmissione dei dati all'interno dei meccanismi IoT[218]. O ancora, l'utilizzo di tecniche di *big data analysis* basate su algoritmi *machine learning* consente di ricavare molte più informazioni dai dati raccolti dai sistemi IoT, che acquisiscono così maggior valore

[216] Chris Nuttall "UK tech rules may single out Facebook, Google", (8 dicembre 2020), *Financial Times,* accessibile da https://www.ft.com/content/4a66cb73-8c30-4117-a4f7-d5de18f0e66b.
[217] Gruppo di esperti del MISE sull'Intelligenza Artificiale, (n. 122), 11-12.
[218] ENISA, "Guidelines For Securing The Internet Of Things, Secure supply chain for IoT", (2020), accessibile da https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things, 33.

commerciale. La creazione di un nuovo quadro normativo non può non tenere conto dell'interdipendenza fra le varie tecnologie, dovendo guardare a soluzioni trasversali e compatibili con le peculiarità di ciascuna. Dall'altro lato, proprio attraverso l'integrazione fra le varie tecnologie sarà possibile studiare le migliori soluzioni applicabili ai singoli casi e in grado di garantire un maggior livello di *compliance* della disciplina.

A questo deve necessariamente accompagnarsi la ridefinizione dei meccanismi di *governance* dei dati, nonché lo sviluppo di infrastrutture e tecnologie che ne consentano la raccolta e la conservazione in modo sicuro, preservandone la qualità. A tal fine, l'Unione europea deve lavorare allo sviluppo di *cloud* propri, rendendosi indipendente rispetto agli altri attori internazionali[219].

CAPITOLO II

II. Internet of Things, blockchain e *smart contracts*: impatto su tutela dei e concorrenza

In questo capitolo ci si soffermerà dapprima su un'analisi dei sistemi IoT, illustrandone le caratteristiche principali ed il funzionamento, ma soprattutto i rischi determinati da questi ultimi sia in termini di tutela dei dati personali che per la concorrenza. Di seguito verranno invece introdotte la tecnologia *blockchain* e gli *smart contract*, proposti quali soluzioni tecniche idonee ad accrescere i livelli di *compliance* dei sistemi IoT rispetto alla disciplina del GDPR. Oltre ad illustrarne gli elementi fondamentali, ci si soffermerà dunque su tutti gli aspetti rilevanti e potenzialmente problematici alla luce della suddetta disciplina, preliminarmente indispensabili ad introdurre la fase conclusiva dell'indagine, in cui sarà spiegato in che modo e con quali effetti le diverse tecnologie potranno essere utilizzate congiuntamente.

2.1 Sistemi Internet of things

2.1.1 Natura e funzionamento

[219] La necessità di creare *cloud* europei sorge in ragione di problemi che affliggono sia il lato della domanda, che quello dell'offerta. Sotto il primo profilo, a livello europeo il numero di *cloud* presenti è particolarmente basso, specialmente nel settore pubblico, ed esistono notevoli differenze fra gli Stati Membri. Inoltre, i soggetti che sviluppano *cloud* non hanno spesso sufficiente visibilità sul mercato. A ciò si aggiungano i problemi di interoperabilità sofferti dalle imprese. Dal punto di vista dell'offerta, va invece segnalato che i *cloud* europei detengono limitate porzioni di mercato, risultando così dipendenti da providers di Paesi terzi. L'assoggettamento dei service providers europei alla legislazione di Paesi terzi, inoltre, accresce i rischi per cittadini e imprese, soprattutto per quanto concerne la tutela dei dati personali. Infine, la mancanza di un'adeguata regolamentazione fa sorgere dubbi sulla *compliance* fra l'attività condotta dai cloud e i principi europei. (European Strategy of Data). Per tutte queste ragioni, l'UE ha deciso di dare il proprio sostegno al progetto Gaia X, promosso inizialmente fra Francia e Germania. Il progetto, tuttavia, non riguarda la creazione di un'infrastruttura europea – come peraltro sarebbe auspicabile – ma l'introduzione di regole comuni e trasparenti per i cloud già esistenti, che consenta una corretta e facile condivisione dei dati indipendentemente dalla loro fonte. (Stefano Carli, 'Gaia X, così l'Europa inizia a dettare legge sulla Nuvola' *La Repubblica (*30 Novembre 2020) 36)

Il termine *"Internet of things"* è stato adottato per la prima volta nel 1999 da Kevin Ashton, uno dei fondatori del Centro Auto-ID al Massachssets Institute of Technology (MIT)[220], il quale lo descriveva come una realtà in cui Internet e il mondo reale sarebbero stati connessi grazie ad un sistema di sensori e dati trasmessi in tempo reale. Soltanto nei primi anni 2000, tuttavia, il termine ha iniziato a diffondersi e ad essere utilizzato ufficialmente fra i ricercatori, le imprese e gli utenti finali. Non esiste una definizione universale di IoT, ma con questo termine ci si riferisce generalmente ad un sistema di oggetti tra loro connessi e in grado, grazie a speciali sensori, di raccogliere dati dall'ambiente circostante e condividerli. L'elemento innovativo rispetto al passato consiste nell'aver fatto confluire in unico sistema tecnologie già esistenti, utilizzando vari standard di comunicazione per consentirne l'integrazione. La diffusione di questi sistemi sta già cambiando le nostre vite, con un impatto notevole in diversi campi dell'industria, ma anche della sanità e dei trasporti[221]. Si pensi al concetto di *"smart home"*, cioè di case dotate di dispositivi che consentono di monitorare e controllare, ad esempio, i consumi di energia, ma anche delle *smart city*, o ancora di dispositivi in grado di tenere sotto controllo le condizioni di salute e le prestazioni sportive. Osservare più da vicino i settori in cui l'utilizzo delle nuove tecnologie avrà un impatto maggiore è utile anche al fine di comprendere a pieno le preoccupazioni legate alla loro diffusione ed individuare possibili soluzioni a riguardo. I settori protagonisti di questa rivoluzione sono quello finanziario, sanitario, logistico, manifatturiero, dell'energia, agroalimentare. In tutti questi settori, pure molto diversi fra loro, la possibilità di sfruttare grandi quantità di dati consentirebbe un notevole miglioramento delle prestazioni e dei servizi forniti, pur ponendo problemi rilevanti in termini di interoperabilità fra i sistemi, sicurezza, tutela dei dati personali. Per quanto concerne quest'ultimo aspetto, si tenga presente che in tutti i settori citati circolano soprattutto dati personali e l'impatto su di essi sarà sempre maggiore in contesti come *smart home* e *smart city* in cui vi è un monitoraggio continuo degli individui, delle loro abitudini e delle loro caratteristiche.

Avere ben chiara la struttura dei sistemi IoT[222] è indispensabile al fine di analizzare i profili problematici in termini di protezione dei dati personali e diritto della concorrenza. La fase di produzione dei dati,

---

[220]Eleonora Borgia, 'The Internet of Things Vision: Key Features, Applications and Open Issues', (2014), vol. 54 Computer Communications, 3, accessibile da https://www.sciencedirect.com/science/article/pii/S0140366414003168?via%3Dihub.

[221] Rose, Eldridge, Chapin (n. 16), 4. Un numero sempre maggiore di imprese sta investendo nello sviluppo di questi sistemi, tanto che nel 2020 si è giunti ad avere circa 75 miliardi di dispositivi connessi fra loro, con un importante impatto sull'economia. Guardando nello specifico al caso italiano, lo sviluppo dei sistemi IoT potrebbe incidere significativamente sul nostro mercato almeno per due ragioni. Da un lato questi sistemi rappresentano uno degli ambiti elettivi per eccellenza per l'impiego dei sistemi d'Intelligenza Artificiale (AI) e se, come auspicabile, il nostro Paese investirà nella diffusione di queste tecnologie e nel loro impiego da parte delle PMI per svecchiare e migliorare i processi produttivi, sfruttare i sistemi AI consentirà alle nostre imprese di competere sia a livello europeo che globale. Dall'altro lato, l'Italia vanta delle vere e proprie eccellenze nell'industria robotica e manifatturiera, pronte a candidarsi come guida nella costruzione e diffusione di sistemi IoT (Gruppo di esperti del MISE sull'Intelligenza Artificiale, (n. 122), 29).

[222] L'impianto strutturale dei sistemi IoT si articola essenzialmente su tre diversi livelli: 1) livello di connettività base, che include i meccanismi finalizzati a stabilire connessioni logiche fra i sistemi, 2) livello di interoperabilità dei *network*, che include i meccanismi che consentono la comunicazione e lo scambio di messaggi fra i sistemi connessi attraverso reti diverse, 3) il livello di interoperabilità sintattica che, infine, include i meccanismi di comprensione della struttura dei dati scambiati fra e attraverso i sistemi connessi. I *layers* dei sistemi IoT, invece, descrivono le funzioni che vengono svolte da ciascun livello. La struttura concreta

quella di condivisione fra i vari dispositivi e, infine, la produzione di *output* e di nuovi dati, pongono tutte problemi distinti. In primo luogo, i dati vengono spesso prodotti senza che l'utente ne sia effettivamente consapevole, ad esempio mediante sensori in grado di raccogliere informazioni dall'ambiente circostante. Il valore aggiunto dei sistemi IoT consiste proprio nella connessione fra dispositivi diversi, che in questo modo possono condividere dati, ampliando le risorse a loro disposizione e migliorando le proprie prestazioni. In generale, è poi indispensabile avere ben chiaro che lo sviluppo e la diffusione di questi sistemi non può prescindere e, anzi, in qualche misura dipende, dai paralleli sviluppi e parallela diffusione di altre tecnologie, fra cui la *blockchain* e, soprattutto, dell'AI e dell'evoluzione della connessione 5G. Per quello che qui interessa, va posta particolare attenzione al rapporto che intercorre fra IoT, AI e Big Data. È indispensabile, infatti, tenere a mente la stretta relazione fra questi concetti, al fine di comprendere che le riflessioni giuridiche sui sistemi IoT non possono prescindere – ai fini di chiarezza e completezza – dalla contestuale analisi dell'impatto dell'AI e dei Big Data.

Il rapporto fra IoT e AI può essere descritto come un rapporto bi-direzionale, nel senso che la loro integrazione da un lato consente ai sistemi IoT di raggiungere livelli massimi di prestazione e, dall'altro, permette all'AI di avere un impatto più incisivo ed esteso su diversi aspetti della nostra vita. Inoltre, la mole di dati prodotta dai sistemi IoT è tale che potrà essere efficientemente gestita solo grazie a sistemi AI, che assumeranno configurazioni diverse a seconda delle esigenze. Una soluzione a cui si guarda con molto favore, soprattutto per le potenzialità dell'industria italiana in questo settore, è quella di integrare sistemi AI all'interno dei singoli dispositivi, migliorandone le prestazioni in termini sia di raccolta che di analisi dei dati (*embedded AI*)[223]. Imprescindibile è anche il legame che esiste fra AI, IoT e Big Data[224]. Come detto, infatti, i sistemi IoT si caratterizzano proprio per la capacità di produrre immense quantità di dati, alla cui elaborazione è legato il livello di qualità delle prestazioni erogate. Il rapporto fra AI e Big Data si basa anch'esso sul fatto che la prima, soprattutto nel caso dei sistemi *machine learning*, si "nutre" di dati e solo elaborandone enormi quantità è in grado di raggiungere risultati rilevanti; di contro, è possibile estrarre maggior valore dai *datasets* proprio impiegando sistemi AI. Lo stesso discorso può farsi, a maggior ragione, con particolare riferimento ai dati personali, dal momento

del sistema dipende dalla sua complessità e il numero di *layers* individuabili in concreto varia notevolmente a seconda dei servizi e delle funzioni per i quali il sistema è stato programmato. La struttura più semplice include almeno tre *layers*. Il primo integra i sensori e gli attuatori che consentono l'identificazione dei vari dispositivi, l'analisi delle risorse e il controllo dell'esecuzione. Include ad esempio telecamere RFID, *wi-fi*, *bluetooth*, dispositivi GPS etc. Il secondo *layer*, invece, riguarda le attività di comunicazione fra i vari dispositivi e sfrutta tutte le tecnologie in grado di monitorare in tempo reale l'ambiente circostante e raccogliere i dati. Infine, vi è il *layer* applicativo, che consente di processare e analizzare i dati ed assumere decisioni conseguenti. Quest'ultimo è il *layer* con cui in concreto si interfacciano gli utenti. (Pappagallo, Durante, Monteleone, (n. 128), 64).

[223]Gruppo di esperti del MISE sull'Intelligenza Artificiale, (n. 122), 30. I sistemi *embedded* sono sistemi fisici quali ad esempio sensori, oggetti intelligenti, robot e impianti di automazione. L'Italia è a livello internazionale uno dei Paesi che possiede altissimi livelli di know-how nell'ambito della progettazione e della creazione di componenti hardware e software intelligenti, nonché di sistemi IoT.

[224] Prof. Dr. Mitrou (n. 131), 17-18.

che grazie all'AI è sempre più facile ottenere dati che consentano di identificare un soggetto specifico. A ciò seguono due tendenze fondamentali: la prima è quella di raccogliere quanti più dati possibile, la seconda, invece, quella di riutilizzare i dati per scopi diversi rispetto a quelli per i quali erano stati originariamente raccolti. La natura e le caratteristiche intrinseche ai sistemi IoT incoraggiano queste tendenze, dato che i sistemi di tracciamento da questi impiegati e le tecniche di analisi avanzata utilizzate, consentono di raccogliere dati personali anche non volontariamente ceduti dagli interessati. In ogni caso è importante far presente che il successo e la diffusione delle nuove tecnologie dipenderà molto dal grado di fiducia riposto dagli utenti nella capacità di queste ultime di tutelare pienamente la protezione dei dati.

2.1.2 ***Internet of things* e protezione dei dati personali: analisi sulla compatibilità fra sistemi IoT e GDPR.**

Il diritto alla privacy e alla protezione dei dati personali a livello europeo assumono il rango di diritti fondamentali, come si evince dalle disposizioni di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea del 2000 (riproclamata nel 2007 come parte del Trattato di Lisbona, entrato in vigore nel 2009)[225]. Come più volte ribadito, l'entrata in vigore del GDPR nel 2018 ha rafforzato il *framework* normativo vigente, introducendo nuove regole per garantire una più efficace tutela dei dati personali, con standard identici all'interno di tutto il territorio dell'UE.

Il *considerando 2* del GDPR[226] chiarisce subito che le nuove regole sono strumentali al mantenimento della libertà, della sicurezza e della giustizia nell'UE, mentre il *considerando 9*[227] mette in luce che dal mantenimento di standard di protezione diversi fra gli Stati Membri potrebbero derivare seri rischi per la concorrenza. Se ne evince che, in una certa misura, l'UE ha da sempre riconosciuto un legame fra la tutela dei dati personali e il diritto alla concorrenza, sebbene le relative discipline abbiano mantenuto ambiti di applicazione chiaramente distinti. D'altronde, il *fil rouge* che lega l'intera produzione legislativa dell'UE è dato proprio dall'obiettivo di rafforzare il mercato unico. La stessa Commissione

[225] Parlamento Europeo, Consiglio e Commissione, *Carta dei diritti fondamentali dell'Unione Europea*, C 202/389, 2000, artt. 7 e 8, https://eur-lex.europa.eu/legal-content/IT/AUTO/?uri=celex:12016P/TXT.

[226] GDPR, Considerando 2. *"I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. 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".*

[227] GDPR, Considerando 9 "[…] *La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione."*

ha di recente ribadito[228] che il fine del GDPR, al pari del Regolamento (UE) 2018/1807[229] sulla circolazione dei dati non personali, è quello di consentire alle imprese di operare a condizioni eque all'interno del mercato, concorrendo a pari armi con quelle stabilite al di fuori del territorio UE. Si ritiene, infatti, che il nuovo diritto alla portabilità dei dati, congiuntamente alla ricerca da parte dei consumatori di soluzioni che garantiscano pienamente la tutela dei dati personali, possa ridurre il rischio di creazione di barriere all'entrata del mercato, favorendo una crescita basata su fiducia e innovazione. In questo senso si apprezza anche l'attività condotta da diverse Autorità antitrust europee, che si sono impegnate nell'aiutare soprattutto le PMI nell'implementazione di misure idonee a garantire la tutela dei dati.

Nel cercare di comprendere se e in che misura lo sviluppo dei sistemi IoT possa dirsi compatibile rispetto alla disciplina del GDPR, un'altra considerazione preliminare di fondamentale importanza è espressa invece dal già citato *considerando 15*[230], che ne mette in luce la natura di strumento "tecnologicamente neutro". In altri termini, il legislatore europeo ha chiarito che la tutela dei dati personali non può e non deve rappresentare un ostacolo allo sviluppo e all'innovazione della tecnologia, né può dipendere dal tipo di tecnologia che viene impiegata. Per questo motivo si è volutamente evitato di adottare termini strettamente tecnici o riferibili nello specifico ad una determinata tecnologia, prediligendo piuttosto un linguaggio neutro e in grado di adattarsi facilmente ai nuovi sviluppi[231]. Si è trattato di una scelta sicuramente lodevole, premiata dalla constatazione che, sebbene in questi anni la tecnologia abbia fatto passi da gigante e il contesto in cui le regole sulla protezione dei dati trovano applicazione sia cambiato radicalmente, il GDPR si sia dimostrato uno strumento legislativo più che adeguato alle nuove emergenti esigenze. La Commissione infatti ha manifestato soddisfazione nel constatare che, nei primi due anni di applicazione del GDPR, questi obiettivi sono stati raggiunti con successo, seppure riconoscendo che le sfide da affrontare nel futuro prossimo riguardano proprio la capacità di conciliare la disciplina in esame con le nuove tecnologie emergenti fra cui, oltre che IoT, *blockchain* e AI[232]. E' stata ribadita la necessità di adottare un regime di protezione dei dati personali sufficientemente flessibile, in grado cioè di adattarsi alle nuove esigenze poste dallo sviluppo tecnologico, muovendo dalla considerazione che il diverso utilizzo dei dati personali richiede inevitabilmente l'adozione di regole e approcci diversi[233].

---

[228] Comunicazione della Commissione al Parlamento Europeo e al Consiglio, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, COM(2020) 264 final, 8-9.

[229] Regolamento (UE) 2018/1807 del Parlamento Europeo e del Consiglio relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, [2018], L 303/59, accessibile da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1807&from=LT.

[230] GDPR, considerando 15.

[231] Prof. Dr. Mitrou, (n. 131), 26.

[232] Commissione, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati* (n. 228), 10-17.

[233] Cate, Mayer-Schonberger, (n. 125), 69-70.

A. Ambito di applicazione del Regolamento (UE) 2016/679

La privacy di gruppo

I sistemi IoT pongono anzitutto un problema di incertezza nella definizione dell'ambito di applicazione materiale del GDPR, identificato con il trattamento dei dati personali sia automatizzato che no[234]. Nello specifico, vengono qui in rilievo i problemi di cui si è già dato atto in termini generali trattando dei Big Data relativi alla protezione del gruppo e non del singolo individuo. In altre parole, si sostiene che la nozione di soggetto interessato andrebbe estesa al fine di includere non solo e non tanto i singoli, quanto le categorie di soggetti destinatari delle decisioni assunte dai sistemi IoT. Infatti, l'impatto di queste ultime sui singoli individui prescinde dalla loro individuazione in quanto tali, essendo esclusivamente legata alla suddivisione di questi in macro-categorie, con il fine ultimo di includerli o escluderli dall'erogazione di specifici servizi e/o differenziare le modalità di fruizione degli stessi[235]. Non essendovi identificazione e non potendosi dunque parlare di soggetto interessato nel significato attualmente previsto dal GDPR, la relativa disciplina non troverebbe applicazione, fallendo evidentemente nel raggiungimento del proprio obiettivo ultimo, ossia quello di garantire il pieno controllo al singolo sui propri dati personali e, soprattutto, assicurargli la più ampia tutela possibile.

La questione verte sul fatto che le decisioni di cui i singoli sono destinatari, pur non basandosi su dati personali – ossia su dati ad essi riconducibili – hanno comunque un impatto diretto su di loro. Stando alla disciplina attuale, tuttavia, il singolo non ha a disposizione mezzi per potersi opporre a tali decisioni, non potendo invocare a propria difesa la disciplina relativa alla tutela dei dati personali. **Quanto attualmente previsto dal GDPR relativamente ai poteri attribuiti alle organizzazioni e/o associazioni rappresentative di determinate categorie di soggetti interessati di agire in nome e per conto di questi ultimi per farne valere gli interessi collettivi non sono sufficienti nel contesto che si sta qui esaminando.** I gruppi a cui qui ci si riferisce, infatti, non sono socialmente riconosciuti né individuabili in maniera evidente. Si tratta di categorie create dai dispositivi stessi sulla base degli algoritmi dai quali sono regolati e ai quali i singoli non hanno neanche piena consapevolezza di appartenere. La direzione più auspicabile, dunque, è quella di un ripensamento della nozione di dato personale e di soggetto interessato, in maniera tale da assicurare protezione effettiva al gruppo[236].

Per comprendere meglio la portata del problema, si ponga l'esempio di una *smart city*, nella quale i vari dispositivi connessi fra loro raccolgono continuamente i dati riconducibili allo stile di vita e alle abitudini degli abitanti. Si pensi, ad esempio, che i suddetti dati vengano poi utilizzati per differenziare il modello

[234] GDPR, Art. 2, comma 1.
[235] Pappagallo, Durante, Monteleone (n. 128), 67.
[236] Mantelero, (n. 129), 245-246; Sandra Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", 2018, vol. 10/no. 2 *Law, Innovation and Technology*, 281, accessibile da https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1527479.

di gestione di raccolta dei rifiuti e/o la quantificazione delle imposte ad essi relative. Si tratta senza dubbio di misure che hanno un impatto diretto sul singolo, e che pure non sono assunte esclusivamente sulla base dei suoi dati personali, ma tenendo in considerazione anche dati aggregati riconducibili ad altri soggetti, parti di un insieme indefinito salvo per, ad esempio, la collocazione geografica (quartiere, macro-area, etc.). In altre parole, i dati così raccolti e analizzati conducono non tanto all'identificazione di un soggetto specifico, quanto a quella del "soggetto-tipo" appartenente ad un determinato gruppo[237] (ad esempio, abitanti di un quartiere borghese con elevato background culturale oppure quartiere eminentemente operaio). In virtù di tale classificazione, il singolo potrebbe tuttavia subire delle conseguenze, anche di natura discriminatoria. Sebbene in virtù di quanto disposto dall'art. 15 del GDPR il singolo ha diritto di accedere ai dati personali oggetti di trattamento, in tal caso tale diritto non potrebbe trovare piena attuazione, poiché a questo andrebbero comunicati dati appartenenti ad altre persone. Un discorso simile potrebbe farsi anche con riguardo ai cosiddetti "veicoli intelligenti", in grado di raccogliere per lo più dati relativi allo stile di guida e al comportamento degli automobilisti. Anche in questo caso i veicoli connessi fra loro scambiano dati appartenenti a soggetti diversi al fine di creare un profilo astratto che definisca un modello di riferimento. Alla pari di quanto appena osservato in relazione alle *smart city*, dunque, a venire in rilievo sono dati che riguardano ***la privacy del gruppo*** e non del singolo. Si coglie dunque il limite dell'attuale definizione di soggetto interessato, che potrebbe condurre ad un insperato conflitto fra diverse posizioni soggettive. Al contrario, introducendo il concetto di ***privacy di gruppo*** questi problemi potrebbero più facilmente trovare soluzione.

L'identificazione del soggetto.

Specularmente al problema appena analizzato, si pone la questione relativa all'identificazione del soggetto. Anche in questo caso il problema è riconducibile a quanto si è già discusso trattando in generale dei Big Data. Si è già dato atto, infatti, del pericolo di re-identificazione legato alla combinazione di dati appartenenti a *datasets* diversi, e ai pericoli che ne conseguono in termini di inefficacia delle tecniche di anonimizzazione finora utilizzate. Si è altresì anticipato che per far fronte a questo problema si è proposto di estendere la nozione di dato personale, sulla base dell'assunto che qualunque dato può, in determinate circostanze e se adeguatamente trattato, condurre all'identificazione di un soggetto specifico. Questo discorso è valido a maggior ragione nel contesto dei sistemi IoT, caratterizzati appunto dalla raccolta su base continua di dati, scambiati fra i vari dispositivi che compongono il sistema. Ne consegue che tutti i dati raccolti siano almeno potenzialmente "riferiti a" un determinato soggetto, o che sia quantomeno molto difficile eliminare con certezza e sin dall'inizio tale possibilità.

[237] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", 289.

Ancora una volta può qui utilmente chiamarsi in causa l'esempio della *smart city*[238]. E' possibile, ad esempio, combinare i dati relativi al tracciamento dei percorsi effettuati con quelli concernenti i posti o i locali frequentati, giungendo non soltanto all'identificazione di un soggetto preciso, ma alla costruzione di un profilo dettagliato di quest'ultimo, in grado di rivelare altresì dati appartenenti alla categoria dei dati speciali ai sensi dell'art. 9 del GDPR.

La "household exception"

A proposito dell'ambito di applicazione materiale definito dall'art. 2 del GDPR, è altresì doverosa una riflessione su quanto stabilito ai sensi della lett. c) dell'articolo circa la non applicabilità della disciplina ivi dettata alle attività condotte a scopo meramente personale o domestico. Il *business model* dei sistemi IoT presuppone che i dati raccolti siano sempre trasferiti ad un altro soggetto o dispositivo, pertanto la deroga in esame non dovrebbe mai trovare applicazione. A ciò si aggiunga il fatto che in molte circostanze vengono raccolti dati appartenenti a soggetti che di fatto neanche utilizzano i dispositivi, come accade ad esempio per i dati raccolti in una *smart city*. Ai fini dell'applicabilità della disciplina non rileva tuttavia la proprietà del dispositivo che raccoglie i dati, quanto che vi sia il trattamento di dati personali[239].

Ambito di applicazione territoriale

La diffusione dei sistemi IoT potrebbe porre dei problemi anche per quanto concerne l'ambito di applicazione territoriale del GDPR. Ai sensi dell'art. 2 sono soggetti all'applicazione della disciplina sulla tutela dei dati personali tutti coloro che si trovano all'interno del territorio dell'UE o che, pur essendo stabiliti altrove, vi svolgano le proprie attività, nonché coloro nei confronti dei quali la disciplina degli Stati Membri troverebbe applicazione in virtù delle norme di diritto privato internazionale. Il GDPR impone altresì che lo stesso livello di tutela sia garantito ai cittadini europei nel caso di trasferimento dei loro dati personali verso Paesi terzi, costruendo a tal fine un complesso sistema basato sulle cosiddette decisioni di adeguatezza ("adequacy decisions") e sulle clausole contrattuali standard (contractual standard caluses)[240]. E' ben possibile infatti, e lo sarà sempre più a mano a mano che la

[238] Ibid, 292.
[239] Art. 29 WP, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", 6.
[240] Si tenga presente a tal proposito la rilevanza della decisione assunta di recente dalla CGUE nell'ambito del caso Schrems II. Il cittadino tedesco Maximilian Schrems, dopo avere già una volta denunciato l'illegittimità della decisione di adeguatezza che regolava il trasferimento dei dati dall'UE verso gli USA (cosiddetto Safe Harbor), si sia rivolto nuovamente alla Corte dell'UE per chiedere l'annullamento anche dalla nuova decisione di adeguatezza adottata fra gli Stati (EU-USA Privacy Shield). La vicenda giudiziaria si è conclusa nel luglio 2020, a seguito del rinvio pregiudiziale della questione alla CGUE, che ha annullato la decisione di adeguatezza. La Corte ha infatti stabilito che i poteri di ingerenza sui dati personali degli individui riconosciuti allo Stato dalla disciplina statunitense si pongono in contrasto con i principi del GDPR. Al tempo stesso la Corte ha però riconosciuto la legittimità delle clausole contrattuali standard, che in questo momento rappresentano dunque lo strumento mediante il quale è regolato il trasferimento dei dati fra i due Paesi. (C-311/18 *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems* [2020] CGUE).
A maggio 2021, la Commissione Europea ha inoltre dichiarato di volere intraprendere un'indagine contro Facebook per presunta violazione dell'art. 102 TFUE. A parere della Commissione, infatti, Facebook sarebbe responsabile di distorcere la concorrenza sul

tecnologia continuerà a svilupparsi, che alcuni dei dispositivi parte di un sistema IoT si trovino al di fuori del territorio europeo. La Commissione ha già evidenziato l'importanza di studiare nuove soluzioni sotto questo profilo ed ha già intrapreso i lavori per l'elaborazione di nuove clausole standard che consentano il trasferimento dei dati verso Paesi terzi nel rispetto della disciplina del GDPR[241]. Tale strumento è parso infatti il più idoneo ad assicurare il mantenimento di standard qualitativi idonei in tempi relativamente veloci. Anche sotto questo profilo un intervento da un punto di vista tecnico ancor prima che normativo, favorirebbe la diffusione e condivisione di regole comuni anche nei territori extra-UE, consentendo un effettivo rispetto della disciplina e la piena tutela dell'interessato. Come si vedrà meglio nel corso del capitolo III, l'integrazione fra sistemi IoT e *blockchain* potrebbe rappresentare il mezzo idoneo a consentire l'attuazione di regole comuni.

B. I princìpi e i diritti dell'interessato

Il principio di liceità e le basi giuridiche del trattamento

a) Il consenso

Si è già detto che l'art. 5 del GDPR include fra i principi che trovano applicazione nel caso di trattamento dei dati personali il principio di liceità, in virtù del quale il trattamento dovrà essere giustificato dalla sussistenza di una delle basi giuridiche individuate dal successivo art. 6. I sistemi IoT non sono immuni ai dubbi sulla validità del consenso quale base giuridica idonea a legittimare il trattamento.

La questione non è chiara ed è ulteriormente complicata dalla difficoltà già discussa in precedenza nel distinguere nettamente i dati personali da quelli non personali.

Perché il consenso possa dirsi liberamente prestato è necessario che il soggetto possa ritirarlo in qualunque momento senza subire alcun detrimento o danno. Dal momento che la qualità dei servizi offerti dai sistemi IoT è direttamente correlata alla mole e alla tipologia di dati che questi possono elaborare, è possibile dire che gli utenti non sarebbero in alcun modo danneggiati dalla scelta di ritirare il proprio consenso? Privando i sistemi della materia prima di cui si nutrono, si rischia infatti di inficiarne il funzionamento. Ciò potrebbe avere degli effetti particolarmente distruttivi nel caso di imprese aventi a disposizione *datasets* limitati, poiché il ritiro del consenso da parte anche di uno solo degli utenti avrebbe potenzialmente un impatto notevole[242]. A monte del problema va tenuto presente che in alcuni casi l'utente potrebbe addirittura non essere consapevole di interagire con un dispositivo "connesso", mancando così del tutto il presupposto fondamentale perché possa consapevolmente prestare il proprio

mercato della pubblicità, consentendo ai propri utenti – attraverso il servizio Marketplace – di vendere ed acquistare prodotti senza il pagamento di costi aggiuntivi. (Javier Espinoza, "Brussels to open formal antitrust probe into Facebook", The Financial Times, (Bruxelles, 26 maggio 2021), accessibile da https://www.ft.com/content/3750ad46-04c3-4010-9fc1-fe2427c8520c).

[241] Commissione, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, (n. 228), 17.

[242] Prof. Dr. Mitrou, (n. 131), 40.

consenso[243]. Basti qui richiamare, ancora una volta, gli esempi delle *smart city* e dei veicoli interconnessi[244]. Nel primo caso infatti i dati vengono raccolti da dispositivi collocati in un'area pubblica, senza che i singoli ne siano consapevoli e/o a conoscenza. Nel secondo caso, invece, sebbene il consenso possa essere prestato dal proprietario del veicolo (che presumibilmente sarà anche il conducente), non può dirsi lo stesso per i soggetti che vi entrano in contatto in qualità di passeggeri o che lo guidino occasionalmente.

In secondo luogo il consenso prestato dall'interessato dovrà essere informato e, con specifico riguardo ai sistemi IoT, ciò implica la capacità degli utenti di comprendere appieno il modo in cui vengono condivisi i dati fra i vari dispositivi, i vari utenti e gli altri titolari del trattamento[245]. La tutela dei dati personali è infatti collegata anche alla fiducia che gli utenti possono riporre nella sicurezza delle comunicazioni fra i dispositivi che costituiscono il sistema e al potere di esprimere proprie preferenze sull'accesso ai dati da parte dei singoli dispositivi, nonché sui terzi con i quali i dati vengono scambiati. Si tratta di un complesso di informazioni difficili da fornire preventivamente e, anche in questo caso, suscettibili di evolversi in modo imprevedibile nel corso del tempo e a mano a mano che il servizio viene erogato. A questi inconvenienti va aggiunto il fatto che, a norma del GDPR, le informazioni debbano essere fornite in modo chiaro e con un linguaggio facilmente comprensibile dall'utente. È dubbia la compatibilità di questi principi con *privacy policy* spesso molto lunghe e ricche di tecnicismi che non solo spesso non vengono comprese, ma addirittura neanche lette dagli stessi interessati.

Per queste ragioni, non sono mancate le proposte di adottare modelli nuovi di consenso, che si discostino dal tradizionale *"notice and consent"* utilizzato fino a questo momento.

L'Information Commissioner's Office (da qui in poi "ICO") – Garante per la protezione dei dati personali nel Regno Unito – ha proposto, ad esempio, di introdurre la possibilità di fornire un consenso graduato[246], mediante l'interazione continua con un *service provider*, in grado di rendere edotti gli interessati delle evoluzioni che mano a mano subisce il trattamento dei loro dati, così che questi possano prestare o meno il proprio consenso in modo consapevole, senza dover restare vincolati ad una scelta tout-court effettuata prima che il trattamento avesse inizio.

Sulla stessa scia si pone la proposta di introdurre un consenso "agile", basato su una previa valutazione relativa ai dati effettivamente necessari per fruire del servizio che consentirebbe all'utente di compiere una scelta razionale e ponderata[247]. Nel caso di dispositivi collocati in un'area pubblica, come accade nel contesto delle *smart city*, questa soluzione risulta comunque limitata, a meno che non venga

[243] Art 29 WP, "Opinion 8/2014 on the on Recent Developments on the Internet of Things", (n. 239), 7.
[244] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (n. 239), 289-290.
[245] Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR" (n. 138), 445; Mantelero, Vaciago, (n.137), 568.
[246] ICO, (n. 163).
[247] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (n. 239), 284.

introdotta la possibilità di limitare la raccolta dei dati soltanto ad utenti specifici. In caso contrario, infatti, ai singoli individui non resta che scegliere se prestare il proprio consenso o evitare del tutto l'area soggetta all'attività di monitoraggio.

La soluzione avallata dall'Art. 29 WP sarebbe piuttosto quella di riconoscere agli utilizzatori un vero e proprio diritto alla disconnessione del dispositivo[248]. Spetterebbe dunque all'utilizzatore decidere se attivarne la connessione, accettandone le condizioni relativamente al trattamento dei dati, nel pieno rispetto dei principi dapprima illustrati.

Su un piano diverso si pone invece l'idea di sostituire il sistema attuale con uno focalizzato maggiormente sui possibili utilizzi dei dati, in cui si prescinda dalle scelte dei singoli, garantendo loro una tutela più ad ampio spettro e, dunque, maggiormente efficace[249]. In questo modo graverebbe sul titolare del trattamento, in qualità di soggetto dotato di adeguate conoscenze e in possesso di informazioni sufficienti a valutare i possibili rischi in termini di tutela dei dati, porre in essere le misure necessarie per prevenirli ed evitarli. Sebbene venga riconosciuta l'importanza di attribuire ai singoli individui il pieno controllo sui propri dati personali, i sostenitori di questo sistema sottolineano che un approccio di questo tipo non è nuovo in contesti nei quali si riconosce la capacità limitata degli individui di assumere delle decisioni consapevoli e ponderate.

b) Il legittimo interesse e l'esecuzione di un contratto

È molto importante, dunque, comprendere se e in che misura le altre basi giuridiche possano costituire delle valide alternative al consenso nel caso dei sistemi IoT.

L'alternativa più accreditata sembra finora essere quella del trattamento basato sul legittimo interesse[250], come si evince anche dalle indicazioni fornite dal Garante italiano per la protezione dei dati personali[251]. Affrontando il tema del trattamento dei dati mediante nuove tecnologie o strumenti automatizzati basato sul legittimo interesse, viene infatti fatto riferimento anche ai dati raccolti nel contesto dei sistemi IoT. Dalle considerazioni ivi svolte emerge con chiarezza che nel fare ricorso a questa base giuridica dovranno tenersi in considerazione molteplici aspetti che ne limitano l'applicabilità. In primo luogo, infatti, la norma dispone che il titolare dovrà accertarsi che non prevalgano le libertà fondamentali dell'interessato e rileveranno comunque le ragionevoli aspettative dello stesso in base alla propria relazione con il titolare. Il provvedimento include fra gli esempi rilevanti il caso in cui l'utente sia cliente del titolare, nonché quello in cui il trattamento sia necessario per garantire la sicurezza o la capacità di

[248] Mantelero, Vaciago (n. 137), 568.
[249] Mayer-Schonberger, Padova, (n. 14), 332.
[250] GDPR, art. 6, lett. f).
[251] GPDP, Provvedimento n. 122 del 22 febbraio 2018 - Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679, accessibile da https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8080493.

una rete. Nel caso in cui il soggetto interessato utilizzi consapevolmente i sistemi IoT, il richiamo alla norma in esame potrebbe rivelarsi utile, potendo dirsi che il bilanciamento di interessi che il titolare è tenuto ad effettuare si risolve positivamente, ossia nel senso di potere affermare che il soggetto interessato poteva ragionevolmente attendersi il trattamento ulteriore. Un discorso diverso deve però farsi nel caso in cui l'interessato non sia consapevole di essere entrato in contatto con un dispositivo connesso, e l'esempio più evidente è dato ancora una volta dal caso delle *smart city*.

Con riferimento a questa ipotesi si tenga inoltre presente che il **GDPR esclude il ricorso al legittimo interesse quale base giuridica valida nel caso in cui il trattamento sia svolto da un'autorità pubblica in esecuzione dei propri compiti.**

Molto importante evidenziare alcuni degli elementi che il titolare dovrà tenere presenti nel valutare se il ricorso al legittimo interesse leda o meno i diritti dell'interessati, fra cui rientrano l'individuazione degli scopi specifici per cui è effettuato il trattamento, la qualità dei dati che vengono trattati, il rispetto dei principi di minimizzazione e sicurezza, quest'ultimo direttamente riconducibile al principio di *privacy-by-design*. Ciò che qui preme sottolineare è che il Garante abbia suggerito di studiare soluzioni che intervengano già nella fase di progettazione, al fine di assicurare il rispetto di questi profili. Si tratta di una delle questioni che potrebbe trovare soluzione proprio grazie all'integrazione dei sistemi IoT con altre tecnologie, quali ad esempio la *blockchain*, note per l'elevato livello di sicurezza che garantiscono.

Inoltre, il legittimo interesse non dovrebbe trovare applicazione laddove sia più idoneo ricorrere ad una diversa base giuridica, quale ad esempio l'esecuzione di un contratto o di misure precontrattuali[252].

Ancora una volta occorrerà distinguere a seconda del contesto e del tipo di dispositivo che viene utilizzato, al fine di comprendere se il trattamento avvenga o meno in virtù di un rapporto contrattuale esistente fra l'interessato e il titolare.

Principio di trasparenza e le sue estrinsecazioni

Il principio di trasparenza sancito dall'art. 5 del GDPR ha diverse estrinsecazioni e impone di porre attenzione a profili diversi in base al contesto specifico in cui si procede al trattamento dei dati.

a) Il diritto d'informazione

[252] GDPR, art. 6, lett. b).

Nel caso dei sistemi IoT gli utenti sono chiamati a riporre fiducia non solo nei singoli dispositivi che compongono il sistema, ma anche nel modo in cui questi comunicano e scambiano i dati fra loro[253]. La mancanza di trasparenza pone inoltre dei problemi che trascendono l'ambito specifico della tutela dei dati personali, potendo questa costituire un serio ostacolo allo sviluppo e all'innovazione. Il rispetto di tale principio coinvolge sia i produttori che i titolari del trattamento, in quanto i primi avranno l'onere (e l'obbligo) di studiare soluzioni *privacy-friendly*, migliorando la tecnologia esistente, mentre i secondi dovranno informare adeguatamente i soggetti interessati[254].

Quanto al primo profilo, emerge ancora una volta la potenzialità derivante dall'integrazione fra le reti IoT e la tecnologia *blockchain*, caratterizzata proprio dall'assoluta trasparenza delle transazioni effettuate sulla catena.

Il secondo aspetto si ricollega invece al diritto di informazione di cui gode l'interessato ai sensi degli art. 13 e 14 del GDPR. Il trattamento non dovrebbe infatti avere inizio se non è possibile fornire all'interessato tutte le informazioni necessarie perché ne comprenda pienamente tutti gli aspetti e sia reso ben consapevole degli eventuali rischi in cui incorre. Ai sensi dell'art. 12 del GDPR, l'informativa dovrà pervenire all'interessato secondo le modalità ritenute maggiormente idonee dal titolare. Nel valutare quali misure possano ritenersi appropriate o meno, il titolare deve tenere conto, fra le altre cose, anche del modo in cui interagisce con l'interessato[255]. In alcuni casi, dunque, l'informativa potrà essere fornita anche direttamente mediante il dispositivo utilizzato dall'utente, fermo restando che le informazioni non dovranno essere eccessivamente complesse e comunque fornite utilizzando un linguaggio chiaro e comprensibile.

Adempiere agli obblighi di informazione imposti dal GDPR potrebbe però collidere con il rispetto di altre disposizioni di legge, comportando ad esempio la divulgazione di segreti commerciali o la violazione dei diritti di proprietà intellettuale. Alla pari, ragioni di pubblico interesse potrebbero ostacolare la divulgazione delle informazioni. Come più volte accennato, l'esatta individuazione del titolare e del responsabile del trattamento pone dei problemi, con la conseguenza che già sotto questo profilo la possibilità di garantire con certezza il rispetto di tale principio appare incerta. Come si vedrà meglio a breve, parimenti problematiche risultano l'individuazione delle finalità specifiche del trattamento e dei terzi con cui i dati saranno condivisi, dal momento che tali sistemi si basano proprio sull'interconnessione fra più dispositivi e sullo scambio continuo e reciproco di dati, così com'è problematico accertare in anticipo se i dati saranno trasferiti verso Paesi terzi, poiché non vi è certezza del luogo in cui si trovino tutti i dispositivi che entrano a far parte del sistema.

[253] Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR" (n. 138), 438.
[254] Prof. Dr. Mitrou, (n. 131), 55-59.
[255] GPDP, Provvedimento n. 122 del 22 febbraio 2018, (n. 251).

b) Il diritto di accesso

Le stesse informazioni che il soggetto interessato ha diritto di ricevere ai sensi degli artt. 13 e 14 del GDPR, potranno essere richieste da quest'ultimo ai sensi del successivo art. 15, che gli attribuisce il cosiddetto diritto di accesso. L'esercizio di tale diritto può essere limitato o addirittura negato da parte del titolare del trattamento qualora ciò comporti l'accesso ad informazioni relative ad individui diversi dall'interessato. In altre parole, quest'ultimo ha diritto ad accedere soltanto ai dati che lo riguardano personalmente, ma non potrà esercitare alcun potere su quelli di altri soggetti. Si è però già messo in luce che tale limitazione rappresenta una vera e propria lacuna nel contesto dei sistemi IoT, laddove emerga il tema della cosiddetta privacy di gruppo[256].

c) Le decisioni automatizzate

Problemi ulteriori sono posti dall'applicazione dell'art. 22, anch'esso estrinsecazione del generale principio di trasparenza. La norma vieta che l'interessato sia soggetto ad una decisione basata unicamente sul trattamento automatizzato dei dati, se questa è idonea a produrre effetti giuridici o comunque ad incidere significativamente su di lui. Nel definire il concreto ambito di applicazione della disposizione acquisisce un ruolo cruciale l'utilizzo del termine "unicamente" [257]. Stando alla lettera della norma, ad escludere la sua applicazione sembrerebbe infatti sufficiente un qualunque intervento umano nel corso del processo decisionale. Nella prassi, soprattutto con riguardo a decisioni che abbiano un'efficacia legale o un effetto comunque significativo per l'interessato, è frequente che vi sia il coinvolgimento di un agente umano almeno in una delle fasi del processo, ma questo è meno vero se si guarda a meccanismi decisionali che presuppongono l'impiego di algoritmi in quanto, anche se formalmente utilizzati come supporto, tali sistemi tendono ad agire in totale autonomia. Bisogna chiarire, dunque, entro quali limiti la partecipazione di un soggetto umano possa di fatto precludere l'applicazione della norma. A tal riguardo l'Art. 29 WP ha riportato delle riflessioni interessanti[258], ponendo l'accento sulla reale influenza che il soggetto coinvolto nel processo decisionale esercita sul sistema. Se l'intervento umano non esercita alcuna influenza sull'*output* finale, limitandosi a confermare la decisione elaborata dal sistema automatizzato, questa rientrerà a pieno titolo nell'ambito di applicazione della norma in esame. Affinché possa effettivamente apportare un cambiamento sulla decisione, il soggetto coinvolto dovrà possedere l'autorità e la competenza necessarie. Anche questo elemento dovrà pertanto essere valutato ai fini dell'applicabilità della disciplina. Posto che la DPIA è individuata come lo strumento migliore per svolgere un'indagine in questi termini, rimane da chiarire se il concetto di "unicamente" vada interpretato dal punto di vista del titolare del trattamento o dell'interessato oppure,

[256] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (n. 239), 281.
[257] Veale, Edwards, (n. 160), 400 e Prof. Dr. Mitrou, (n. 131), 68.
[258] Art. 29 WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", (n. 159), 20.

come forse sarebbe più conveniente, secondo una valutazione quanto più imparziale ed oggettiva possibile[259].

Un altro profilo di incertezza sui confini di applicabilità dell'art. 22 è dato dal riferimento agli "effetti significativi" che le decisioni in questione devono produrre sull'interessato. A differenza degli effetti legali, chiaramente limitati alle ipotesi in cui la decisione determini un cambiamento degli obblighi e dei diritti che fanno capo all'interessato, non è chiaro cosa rientri nella nozione di effetti significativi. Le linee-guida dell'Art. 29 WP[260] includono in questa categoria le decisioni in grado di influenzare le circostanze, il comportamento o le scelte dell'individuo, nonché quelle che possono determinare l'esclusione o la discriminazione dello stesso. Tale formulazione sembrerebbe suggerire che anche nelle ipotesi in cui la decisione finale sia di fatto lasciata all'individuo, se nel corso del processo vi sono state delle statuizioni intermedie che hanno comunque avuto un'influenza determinante, la norma potrebbe trovare applicazione. Un esempio tipico potrebbe essere quello di sistemi di profilazione che danno vita al fenomeno dei prezzi differenziati. Sebbene la scelta di acquistare o meno un prodotto rimanga comunque in capo al consumatore finale, la sua decisione sarà inevitabilmente influenzata dall'offerta che gli è stata proposta, risultato dell'algoritmo utilizzato.

Discostandosi dall'interpretazione prevalente nel periodo di vigenza della Direttiva 95/46/EC, l'art. 29 WP ha inoltre incluso fra le decisioni soggette all'applicazione dell'art. 22 tanto quelle che hanno effetti negativi sull'individuo, quanto quelle aventi un impatto positivo. Sul punto si è aperto un dibattito[261] con riferimento agli annunci pubblicitari personalizzati, dividendo chi ritiene che siano qualificabili come decisioni automatiche ai sensi dell'art. 22 e chi invece ritiene che non costituirebbero delle vere e proprie decisioni, potendo comunque essere bloccati o ignorati.

L'Art. 29 WP, assumendo una posizione intermedia, ha definito i criteri da valutare al fine di affermare che le pubblicità "targettizzate" non solo siano delle decisioni, ma abbiano anche un effetto significativo sull'interessato. Restano esclusi da tale nozione gli annunci che si basano genericamente sul genere, l'età o la città di provenienza, mentre si dovranno analizzare il livello di intrusività della profilazione, le aspettative e i desideri dei singoli individui, le modalità con cui l'annuncio è trasmesso, il fatto che i destinatari siano soggetti particolarmente vulnerabili. Tali criteri, mutuati per lo più dalla disciplina sui consumatori, non sono tuttavia dirimenti nel determinare se le offerte targettizzate abbiano o meno un effetto significativo sull'interessato e la riflessione dell'Art. 29 WP non consente neanche di prendere in considerazione un elemento di fondamentale importanza, ossia l'effetto di "classificazione" creato da tali meccanismi, alla pari di quanto avviene con i prezzi differenziati, che escludono determinati soggetti

[259] Veale, Edwards, (n. 160), 401.
[260] Art. 29 WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", (n. 159), 21-22.
[261] Veale, Edwards, (n. 160), 401-402.

dal novero dei destinatari di specifiche offerte. Il problema della significatività degli effetti si ricollega inoltre al più generale problema di determinazione dell'ambito di applicazione del GDPR, già ampiamente analizzato, dal momento che ci si interroga sulla possibilità di considerare come significativa una decisione che incida non sul singolo individuo, ma su uno specifico gruppo.

Le linee-guida non forniscono indicazioni rilevanti per valutare se in tal caso l'art. 22 trovi applicazione o meno. Le caratteristiche di un determinato gruppo possono comportare l'assunzione di decisioni significative per un singolo individuo, anche nell'ipotesi in cui i dati su cui tali decisioni si basano siano forniti da un soggetto diverso. Anche in questo caso, non c'è una risposta chiara all'interrogativo sull'applicabilità della norma, anche se non sembrerebbero esservi ostacoli in tal senso. La questione va infatti risolta valutando le conseguenze della decisione sull'individuo, non certo la fonte di provenienza dei dati trattati. Soltanto interpretando la norma in questi termini si potrà infatti garantire tutela effettiva nel contesto dei sistemi IoT e degli algoritmi *machine learning*[262].

La norma non risolve neanche i problemi relativi alle possibili discriminazioni risultanti dall'utilizzo degli algoritmi. L'unico riferimento esplicito in tal senso è al *considerando 71*, a norma del quale il responsabile del trattamento dovrebbe adottare tutte le misure tecniche ed organizzative volte a scongiurare ogni forma di discriminazione basata su dati sensibili nei confronti delle persone fisiche.

Il secondo comma dell'art. 22 illustra alcune circostanze in cui la disciplina dettata dal primo comma non trova applicazione[263]. Fra le deroghe individuate dall'articolo vi sono l'ipotesi in cui la decisione sia necessaria per la conclusione o l'esecuzione di un contratto fra l'interessato e il titolare e quella in cui quest'ultimo abbia prestato il proprio consenso. Il GDPR dispone che in queste ipotesi l'interessato mantenga comunque diritto di ottenere almeno l'intervento umano, di esprimere la propria opinione e di contestare la decisione[264]. Nell'ambito dei sistemi IoT, se da un lato si potrebbe argomentare nel senso di ritenere che le decisioni automatizzate assunte dai dispositivi siano necessarie per il funzionamento stesso del sistema, costituendo così il trattamento dei dati l'esecuzione di un contratto fra l'utente e il titolare del trattamento, meno chiaro è in che modo quest'ultimo potrà garantire i diritti riconosciuti all'interessato dal terzo comma. A ciò si aggiunga, come si vedrà in seguito, che non sempre è agevole individuare chi possa essere qualificato come titolare del trattamento. Alla pari, vengono nuovamente qui in rilievo le considerazioni precedentemente svolte sulla validità del consenso come base giuridica del trattamento. Un'ultima considerazione va fatta avendo riguardo di quanto stabilito dal quarto comma

[262] Ibid.
[263] GDPR, art. 22, comma 2. "Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato".
[264] GDPR, art. 22 comma 3.

dell'articolo[265], che esclude la possibilità che le decisioni automatizzate si basino categorie speciali di dati di cui all'art. 9 GDPR. Il trattamento effettuato mediante l'utilizzo di nuove tecnologie, e soprattutto nel caso di algoritmi *machine learning*, potrebbe consentire di ottenere tali dati pur partendo dal trattamento di altre categorie. Da ciò deriverebbe che ogni qualvolta il titolare possa ragionevolmente ritenere che il trattamento comporti la creazione di categorie speciali di dati, questo debba avvenire nel rispetto della disciplina *ad hoc* dettata dall'art. 9.

Ancora una volta, per assicurarsi di agire legittimamente, il titolare dovrebbe anticipare l'analisi sulla correttezza del sistema alla fase di progettazione[266]. Si tenga inoltre presente che l'art. 22 trova applicazione solo nel momento in cui una decisione è effettivamente assunta, perdendo l'occasione di intervenire a monte del problema, ossia quando vengono definiti i criteri potenzialmente pregiudizievoli su cui essa si basa[267].

Anche la relazione fra l'art. 22 e il diritto d'accesso di cui all'art. 15 è problematica. La lett h) del suddetto articolo, infatti, indica fra gli elementi a cui l'interessato deve avere accesso proprio l'esistenza di un processo decisionale automatizzato. Va da sé che l'incertezza relativa all'ambito di applicazione della disposizione si ripercuote naturalmente anche sulla concreta possibilità per l'interessato di esercitare tale diritto.

Principio di limitazione delle finalità e di minimizzazione

a) Principio di limitazione delle finalità

Il principio di limitazione delle finalità impone che il trattamento avvenga per finalità determinate, esplicite e legittime. Ciò implica che le finalità del trattamento devono essere individuate con certezza prima che questo abbia effettivamente inizio e comunicate all'interessato. Nei sistemi IoT, invece, il contesto nel quale i singoli dispositivi vengono autorizzati alla raccolta dei dati può variare notevolmente rispetto a quello nel quale i dati saranno poi di fatto utilizzati[268]. I dati vengono condivisi e riutilizzati per finalità diverse, con la conseguenza che individuare a priori le finalità concrete del loro utilizzo risulta praticamente impossibile. Fenomeno destinato ad aggravarsi ulteriormente nel caso di sistemi che impiegano la cosiddetta "*embedded* AI", sfruttando le potenzialità dell'Intelligenza Artificiale nella fase di analisi dei dati raccolti. Questo principio è stato oggetto di critiche, in quanto vi è chi ritiene che porrebbe un freno alla libertà delle imprese di innovarsi.

[265] GDPR, art. 22, comma 4. "Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato".
[266] Veale, Edwards, (n. 160), 403.
[267] Prof. Dr. Mitrou (n. 131), 73-74.
[268] Madaan, Mohd, Sastry, (n. 126), 126.

Sul punto si è espresso l'ICO[269], sottolineando che la limitazione delle finalità mira ad impedire l'arbitrario riutilizzo dei dati, ma non deve costituire un limite insuperabile o un principio eccessivamente rigido. Si aprirebbe, dunque, la possibilità per le imprese di trarre valore aggiunto dall'utilizzo dei dati contenuti nei propri *datasets*, sebbene bisogna tenere conto delle circostanze del caso concreto.

Il nodo centrale resta quello di determinare cosa possa essere ritenuto compatibile o meno rispetto alla finalità iniziale, alla luce del *considerando 50* del GDPR[270], che elenca gli elementi da tenere in considerazione nello svolgimento di tale valutazione. A parere dell'ICO[271], il parametro sulla base del quale andrebbe condotta tale indagine è la **correttezza**. Ciò implicherebbe che i dati, se legittimamente raccolti per un determinato fine, potrebbero essere riutilizzati per un fine diverso nella misura in cui questo risulti corretto.

Questa soluzione è stata criticata perché aprirebbe a profili d'incertezza, dal momento che il concetto di correttezza rimane un concetto aperto ad ampia interpretazione[272].

Infine, l'autorità garante per la protezione dei dati personali norvegese ha evidenziato la difficoltà nel marcare la linea di confine che separa il trattamento dei dati a fini statistici o di ricerca e quello per finalità diverse, dal momento che il funzionamento dei sistemi AI si basa proprio sulla rielaborazione e il riutilizzo dei dati[273]. Si noti infine che fra gli elementi a cui il titolare ha diritto di accedere a norma dell'art. 15 del GDPR figurano anche le finalità del trattamento. Se non è possibile individuare con certezza la finalità, anche l'esercizio di tale diritto viene dunque messo in discussione.

b) Principio di minimizzazione

Sebbene limitare la raccolta dei dati al minor numero possibile sia considerata la migliore strategia per garantire pienamente la tutela dei dati personali, alla luce delle considerazioni sin qui svolte è evidente che tale principio si pone in netto contrasto rispetto al connaturato bisogno di dati dei sistemi IoT.

Ai sensi dell'art. 5, comma 1, lett. c) del GDPR, il titolare del trattamento deve dimostrare che i dati raccolti siano soltanto quelli assolutamente necessari. Nel caso dei sistemi IoT, pertanto, quest'ultimo

[269] ICO, (n. 163), 37.
[270] GDPR, considerando 50. "[…]Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto".
[271] ICO, (n. 163), 38.
[272] Butterworth, (n. 166), 260.
[273] Prof. Dr. Mitrou, (n. 131), 48.

dovrà dimostrare la sussistenza di un nesso causale fra la raccolta dei dati e il prodotto o il servizio offerto all'interessato, non potendosi ammettere la raccolta dei dati finalizzata esclusivamente alla loro conservazione[274].

Tale principio potrebbe dunque rappresentare un serio ostacolo all'adozione e alla diffusione di questi sistemi, poiché ne pregiudica il funzionamento ottimale. Nella maggior parte dei casi, infatti, i dati raccolti dai sistemi IoT non sono immediatamente ed esclusivamente utilizzati per consentire la fruizione del servizio o la disponibilità del prodotto, quanto per il loro miglioramento, inteso anche come la personalizzazione degli stessi. Tenendo conto dell'incidenza che la raccolta dei dati ha sui diritti fondamentali della persona, il titolare del trattamento dovrà valutare se il principio di proporzionalità sia stato rispettato o meno[275]. Per tutte queste ragioni il principio di minimizzazione è considerato come un ostacolo allo sviluppo dei nuovi sistemi, ponendosi in significativo contrasto con il loro meccanismo di funzionamento di base.

Principio di esattezza e diritto alla rettificazione dei dati

In virtù del principio di esattezza, il titolare del trattamento deve assicurare che i dati trattati siano sempre corretti e aggiornati in riferimento alla finalità specifica del trattamento. A questo principio è riconducibile il diritto alla rettificazione dei dati. Nel contesto dei sistemi IoT, il rispetto di tale principio pone in capo agli sviluppatori e ai programmatori l'onere di predisporre meccanismi adeguati di aggiornamento dei propri *datasets* e di verifica dell'identità degli utenti che usufruiscono del servizio[276]. Anche in questo caso, dunque, il rispetto alla disciplina del GDPR si lega alla creazione di soluzioni di natura tecnica. Un esempio, come si vedrà meglio nel capitolo III, potrebbe essere l'utilizzo di un sistema di *smart contract* il processo di verifica e ne garantisca il massimo livello di sicurezza.

Principio di sicurezza e privacy-by-design

L'art. 5 impone infine al titolare del trattamento di porre in essere tutte le misure ritenute idonee a garantire che il trattamento assicuri il più alto livello di sicurezza. Le linee-guida sui sistemi IoT emanate dall'ENISA[277] individuano proprio la tutela dei dati personali come uno dei maggiori problemi giuridici legati alla sicurezza di tali sistemi.

[274] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (n. 239), 273.
[275] Prof. Dr. Mitrou, (n. 131), 49-50.
[276] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (n. 239), 273.
[277] ENISA, "Guidelines For Securing The Internet Of Things, Secure supply chain for IoT", (n. 216).

Per tale ragione l'osservanza e il rispetto principio di *privacy-by-design* già nella loro fase di progettazione e sviluppo è di cruciale importanza[278]. Al fine di raggiungere gli obiettivi sperati, dovrà infatti essere posta adeguata attenzione ai problemi che ogni singola fase di utilizzo dei sistemi pone, cercando di studiare soluzioni *ad hoc* per ciascuna di esse. La sicurezza dei dati è infatti messa a rischio non soltanto nella fase di produzione/raccolta degli stessi, ma anche durante la loro utilizzazione, ad esempio nel corso delle comunicazioni fra i vari dispositivi.

Rileva anche sotto questo profilo la questione relativa all'identificazione dei dispositivi che entrano a far parte del sistema e ai meccanismi di autorizzazione per l'accesso ai dati che possono essere integrati[279]. Gli utenti, infatti, dovrebbero poter riporre piena fiducia nella sicurezza dei dispositivi che compongono il sistema ed essere in grado di esprimere le proprie opzioni sui poteri di accesso ai dati che intendono rilasciare a ciascuno. Il riconoscimento di un potere di questo tipo in capo al singolo presuppone tuttavia che il livello di informazione sia adeguato alle tipologie di dati raccolti, nonché alle modalità di condivisione e analisi degli stessi. Non solo è in concreto molto difficile che si realizzi una situazione di questo tipo, ma inoltre meccanismi di accesso differenziati presuppongono la creazione di un sistema centralizzato che, sebbene garantisca livelli maggiori di sicurezza, pone ulteriori problemi in termini di tutela dei dati. Tali sistemi, infatti, prevedono l'esistenza di un ente centralizzato che abbia il potere di coordinare e gestire la condivisione dei dati fra i vari dispositivi sulla base dei permessi riconosciuti a ciascuno di essi dall'utente. In tal modo, l'entità centrale acquista tuttavia un potere smisurato sui dati condivisi all'interno del sistema, che potranno essere fra loro ulteriormente combinati ed elaborati.

Una delle soluzioni principali suggerite dall'ENISA è data proprio dall'integrazione fra i sistemi IoT e la tecnologia *blockhain* che, caratterizzandosi proprio per la natura di registro distribuito e non centralizzato, rappresenta una soluzione innovativa per innalzare i livelli di sicurezza[280].

Il diritto alla portabilità dei dati

Nel proprio report sul GDPR[281] è la stessa Commissione a fare menzione dei sistemi IoT fra le tecnologie emergenti che enfatizzano l'importanza del diritto alla portabilità dei dati e il suo ulteriore rafforzamento. Anche in questo caso l'effettivo raggiungimento del risultato sperato dal dato normativo è inscindibilmente legato all'adozione di nuove soluzioni tecniche. Il diritto alla portabilità, presuppone infatti l'adozione di protocolli e strumenti di comunicazione che facilitino lo scambio e la circolazione dei dati anche fra dispositivi diversi. In questo senso l'integrazione fra IoT e *blockchain* potrà giocare

[278] Regolamento sulla protezione generale dei dati, art. 25.
[279] Mandaan, Ahad, Sastry, (n. 120), 130-131 e Wachter, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", (n. 138), 438.
[280] ENISA, "Guidelines For Securing The Internet Of Things, Secure supply chain for IoT", (n. 216), 33
[281] Commissione, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, (n. 228).

un ruolo importante, dal momento che i dispositivi connessi alla catena hanno libero accesso ai dati caricati su di essa.

La crescita dell'economia digitale, quale risultato della facilitata circolazione e condivisione dei dati, ha un impatto – come si è detto – tanto sulla disciplina concorrenziale, quanto su quella di tutela dei consumatori[282]. L'art. 20 del GDPR non obbliga i titolari a garantire la piena interoperabilità fra i dati, né tantomeno impone loro l'utilizzo di un formato specifico. Nel rispetto del principio di neutralità tecnologica che permea la disciplina in esame, la disposizione si limita ad imporre al titolare del trattamento l'utilizzo di formati compatibili, bilanciando comunque tale imposizione con il mantenimento di costi sostenibili e dell'evoluzione tecnologica. In questo modo il legislatore limita la propria ingerenza sulla definizione dei modelli di *business* scelti dalle aziende[283]. La questione dell'interoperabilità dei dati diviene ancora più rilevante grazie allo sviluppo delle nuove tecnologie, a maggior ragione se si guarda ai sistemi IoT basati proprio sulla connessione e la condivisione dei dati fra dispositivi diversi. È un aspetto che auspicabilmente dovrebbe essere preso più sul serio, dato che consentirebbe di conciliare il miglioramento dei livelli di prestazione dei sistemi alla tutela dei dati personali e della concorrenza.

La formulazione della norma pone però non pochi problemi di adattamento. In primo luogo, l'esercizio del diritto alla portabilità dei dati è ammesso nella sola ipotesi in cui il trattamento sia basato sul consenso o sull'esecuzione di un contratto[284]. Rimane dunque escluso dall'ambito di applicazione della norma il trattamento basato sul legittimo interesse. La limitazione dell'ambito di applicazione del diritto alle sole due basi giuridiche summenzionate è stata tradizionalmente ricollegata proprio alla sua vocazione commerciale[285]. Dal momento che la finalità ultima della norma, secondo la ratio che il legislatore ha inteso attribuirle, è quella di favorirne la circolazione dei dati, la dottrina ha ritenuto che fosse legittimo limitarne l'operabilità ai trattamenti che si basano sul consenso o sull'esecuzione di un contratto. Come si è già avuto modo di vedere, l'inadeguatezza del consenso come base giuridica ha condotto all'esplorazione di basi ulteriori che potessero legittimare il trattamento dei dati. Fra queste la più accreditata è stata proprio il legittimo interesse. Resta dunque da chiedersi se la tesi sostenuta dalla dottrina per giustificare il limitato ambito di applicazione della norma abbia – e, in caso di risposta affermativa, in che misura - ancora una propria valenza, dal momento che tenendo fede alla formulazione vigente l'applicazione della norma andrebbe esclusa proprio da quei contesti in cui maggiormente potrebbe esplicare la propria utilità.

[282] Battelli, D'Ippolito, (n. 190), 203.
[283] Ibid., 204.
[284] GDPR, art. 20, comma 1, lett. a).
[285] Battelli, D'Ippolito (n. 190), 192.

Un altro aspetto problematico potrebbe essere rappresentato dal fatto che la norma riconosca all'interessato il diritto ad ottenere il trasferimento dei dati "che lo riguardano" direttamente[286]. Ragionevolmente ciò dovrebbe condurre il titolare del trattamento a raccogliere e conservare i dati relativi a ciascun individuo separatamente e non in forma aggregata, seguendo un approccio chiaramente in contrasto rispetto a quello naturalmente incoraggiato dai sistemi IoT[287].

Torna qui in gioco, ancora una volta, la questione relativa alla "privacy di gruppo". Parimenti problematico è l'utilizzo del termine "forniti", che farebbe rientrare nell'ambito di applicazione della norma i soli dati che l'interessato abbia consapevolmente ceduto al titolare[288]. La ratio della disposizione va ricercata nell'esigenza di garantire che i dati coperti da diritti proprietà intellettuale o che siano il frutto di analisi svolte dal titolare non vengano gratuitamente divulgati e fatti circolare. Il termine "forniti" si presta tuttavia a due diverse interpretazioni e accogliendo l'una o l'altra cambiano i confini di applicazione della norma[289].

Secondo la prima interpretazione, solo i dati ceduti direttamente dagli utenti ricadrebbero entro l'ambito di applicazione dell'art. 20. Al contrario, dando un'interpretazione estensiva vi sarebbero inclusi anche quelli raccolti dal titolare senza che vi sia un esplicito consenso dell'interessato. Gli argomenti a sostegno della prima tesi sono molteplici, a partire da quelli deducibili da un'analisi letterale della norma che con l'utilizzo del termine "forniti" presuppone un atteggiamento attivo dell'utente.

Un altro argomento è quello riguardante i costi che il titolare del trattamento sarebbe tenuto a sostenere nel garantire un più esteso diritto alla portabilità dei dati[290]. A sostegno della tesi estensiva soccorre invece il testo del *considerando 68*, il quale ribadisce che il fine della norma è quello di rafforzare il controllo dell'interessato sui propri dati personali e che, specialmente quando il trattamento riguarda l'impiego di nuove tecnologie, debba essere preferita comunque l'interpretazione che garantisce maggiormente l'interessato. A restare fuori dall'ambito di applicazione della norma sono i dati ottenuti dall'analisi svolta dal titolare del trattamento, ai quali si riconosce piena protezione in ossequio alla disciplina sulla proprietà intellettuale[291]. Senza dubbio, inoltre, escludere dall'applicazione della norma

---

[286] Battelli, D'Ippolito (n. 190), 194-199; De Hert, Papakonstantinou, Malgieri, Beslay, Sanchez, (n. 190), 198.

[287] Questo aspetto è strettamente correlato al fatto che i sistemi IoT siano generalmente basati su architetture *cloud*. Problemi ulteriori sorgono anche in relazione al diritto di accesso ai dati che il GDPR riconosce all'interessato, poiché l'accesso e la gestione autonoma degli stessi divengono particolarmente complesse.

[288] De Hert, Papakonstantinou, Malgieri, Beslay, Sanchez, (n. 190), 199-200.

[289] Seguendo un'interpretazione restrittiva, i dati "forniti" sarebbero soltanto quelli trasmessi dall'interessato in forma scritta o comunque in modo esplicito, mentre interpretando estensivamente il termine vi rientrerebbero tutti i dati raccolti previo consenso dell'interessato o sulla base di un accordo contrattuale. Nel contesto delle nuove tecnologie e delle piattaforme digitali, i dati vengono generalmente prodotti secondo tre diverse modalità: possono essere ceduti direttamente dagli utenti o "raccolti" dai titolari mentre questi ultimi usufruiscono dei servizi, oppure dedotti o predetti mediante elaborati sistemi di analisi.

[290] Pur tenendo in considerazione quanto stabilito dal quarto comma dell'articolo, che dispone il bilanciamento del diritto in esame con i diritti e le libertà degli altri, va comunque detto che graverebbe sul titolare l'onere di dimostrare l'effettiva eccessività dei costi.

[291] Battelli, D'Ippolito (n. 190), 198-199.

i dati dedotti o comunque predetti dal titolare riduce il livello di controllo effettivo che la disciplina garantisce all'interessato, dal momento che questi rappresentano una porzione sempre maggiore – e di maggior valore – dei dati che il titolare detiene. L'impostazione adottata è comunque apprezzabile dal momento che i dati "osservati" sono sempre maggiori e destinati ad aumentare proprio con l'avvento di tecnologie come l'IoT. In ogni caso la definizione del concreto ambito di applicazione non potrà prescindere da un'analisi caso per caso che, tenendo conto delle circostanze concrete, consenta di determinare quando un dato possa definirsi "fornito" o meno[292].

Recenti studi[293] dimostrano inoltre che, nonostante il diritto alla portabilità sia vantato come il diritto che garantirebbe maggior controllo all'interessato sui propri dati personali, il concreto esercizio dello stesso, specie nel caso dei sistemi IoT, sia particolarmente difficoltoso.

In primo luogo, dalla comparazione di diverse *privacy policy* è emersa l'esistenza di un problema di tipo informativo, nel senso che gli utenti non ricevono informazioni adeguate circa la possibilità e le modalità di esercizio di tale diritto.

In secondo luogo si è riscontrato un problema di tipo tecnico, ossia di materiale difficoltà nell'ottenere il trasferimento dei dati da un titolare all'altro. Sotto questo profilo è possibile intervenire solo promuovendo lo sviluppo di standard unici e diffusi, nonché sfruttando soluzioni di *privacy-by-design* che consentano di risolvere il problema alla radice[294]. Riguardo lo sviluppo di standard comuni è importante evidenziare che qualora l'UE non intervenga tempestivamente, è forte il rischio che inizi a diffondersi l'utilizzo di standard approvati dai Paesi terzi, ma non conformi alla disciplina del GDPR[295]. Infine, un aspetto certamente non trascurabile è che l'esercizio del diritto alla portabilità dei dati vada comunque bilanciato rispetto ai diritti di eventuali terzi coinvolti, sia nel senso che l'esercizio di tale diritto non può comprimere diritti altrui, sia nel senso che non possa risolversi in un'indebita violazione di diritti di proprietà intellettuale[296]. Il primo profilo include tanto l'ipotesi in cui ai soggetti terzi venga preclusa la possibilità di esercitare i propri diritti, quanto quella in cui si acceda indebitamente a dati di terzi come conseguenza del diritto alla portabilità. Il secondo aspetto, invece, si ricollega alla necessità di tutelare il titolare del trattamento da possibili abusi che comportino la rivelazione di segreti industriali, provocandogli un danno in termini economici. Si osserva che da questo punto di vista la norma

[292] Di fronte ai limiti presentati dal diritto alla portabilità dei dati si fa presente che, laddove questo non sia in concreto esercitabile, all'interessato sarà comunque riconosciuto il diritto d'accesso ai sensi dell'art. 15. Le due norme perseguono però finalità diverse ed è dubbio in che misura l'esercizio del solo diritto di accesso possa considerarsi soddisfacente nell'ottica generale dei principi sanciti dal GDPR.

[293] Sarah Turner, July Galindo Quintero, Simon Turner, Jessica Lis e Leonie Maria Tanczer. "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment" (2020), *New Media & Society*, accessibile da https://journals.sagepub.com/doi/10.1177/1461444820934033.

[294] Urquhart Lachlan, Sailaja Neelima, Derek McAuley, "Realising the Right to Data Portability for the Domestic Internet of Things" (2018), vol. 22, no. 2 Personal and Ubiquitous Computing, 317-318, accessibile da https://link.springer.com/article/10.1007/s00779-017-1069-2.

[295] Turner, Quintero, Turner, Lis, Tanczer. (n. 293), 16.

[296] Battelli, D'Ippolito (n. 190), 209-212.

sembrerebbe fornire una tutela adeguata, nella misura in cui lascia al titolare la libertà di definire il formato in cui cedere i dati, senza imporgli l'obbligo di trasferire informazioni concernenti i meccanismi di funzionamento dei propri sistemi[297].

Diritto alla cancellazione dei dati

Sebbene il cosiddetto "diritto all'oblio" sia stato espressamente riconosciuto dal legislatore solo con l'entrata in vigore del GDPR, la sua elaborazione a livello giurisprudenziale è risalente e strettamente collegata alla nota sentenza *Google Spain*[298] nella quale, argomentando sulla base del controllo che i motori di ricerca esercitano sui propri contenuti, la CGUE stabilì che questi ultimi fossero responsabili nel garantire la cancellazione dei dati. Alcune delle considerazioni svolte dalla dottrina successivamente all'emanazione della sentenza in esame sono tutt'ora interessanti al fine di valutare se e in che misura il rispetto di tale diritto collida con lo sviluppo delle nuove tecnologie[299] e se, per quello che qui interessa maggiormente, possa ostacolare la diffusione dei sistemi IoT.

Uno dei pareri più critici nei confronti del criterio adottato dalla CGUE per determinare chi fosse qualificabile come titolare del trattamento era stato quello espresso dal prof. Oreste Pollicino[300], che definì addirittura inconferente l'argomento adottato dalla CGUE a sostegno di un'interpretazione ampia della nozione di titolare del trattamento, adducendo quale giustificazione la necessità di garantire una più ampia tutela agli interessati. A parere del docente, infatti, l'estensione della responsabilità finirebbe con lo snaturare il modello di *business* degli operatori[301]. Alcune considerazioni sono qui doverose. Si è più volte ribadito, infatti, che il valore dei dati raccolti nell'ambito dei sistemi IoT cresce proporzionalmente alla loro quantità e alla capacità delle imprese di trattarli mediante tecniche di analisi

[297] E' bene analizzare il rapporto che intercorre fra il diritto in esame e il diritto alla cancellazione dei dati sancito dall'art. 17 del GDPR. È lo stesso art. 20 a specificare che il diritto alla portabilità dei dati non può essere esercitato con pregiudizio del diritto alla cancellazione, sancendo la preminenza di quest'ultimo. In altre parole, nel garantire la portabilità dei dati il titolare del trattamento non potrà utilizzare tecniche che precludano in modo definitivo la possibilità di cancellarli. E' bene porre l'accento, infatti, sulla considerazione che il trasferimento dei dati da un titolare del trattamento ad un altro non presuppone la cancellazione dei dati da parte del primo. Il fine della norma è quello, già evidenziato, di favorire la creazione di un ambiente maggiormente interconnesso e interoperabile, operando su un piano diverso rispetto a quello del diritto alla cancellazione. Si coglie proprio in questo l'impatto positivo che il diritto alla portabilità dei dati ha sulla concorrenza, incidendo sulla creazione di posizioni dominanti o addirittura monopolistiche.

[298] CGUE, C-131/12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González [2014].

[299] Silvia Martinelli, "Diritto all'Oblio e Motori Di Ricerca: Memoria e Privacy Nell'Era Digitale", (Vol. 5;5, Milano: Giuffrè, 2017), 174-175.

[300] Oreste Pollicino, "Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain", *Il diritto dell'informazione e dell'informatica*, (2014), fascicoli 4-5, 569 ss.

[301] Altri autori, come Alessandro Palmieri e Roberto Pardolesi, hanno fatto notare che l'atteggiamento della CGUE nei confronti di Google sembra tradire una certa ostilità dettata dalla posizione di vantaggio in cui la piattaforma si trova rispetto agli utenti, dalla quale si vorrebbe far discendere in capo a quest'ultima una responsabilità particolare, sulla falsariga di quanto avviene nella disciplina antitrust. (Alessandro Palmieri, Roberto Pardolesi, "Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google", *Nuovi Quaderni del Foro Italiano*, (Quaderno n. 1, 2014).

dei dati, al fine di ricavarne più informazioni e trarne profitto. Va da sé che la cancellazione dei dati si ponga dunque in netto contrasto rispetto al modello di *business* adottato da tali sistemi. Se le argomentazioni addotte dal prof. Pollicino venissero accolte nell'analisi del contesto attuale, sarebbe difficile ammettere il pacifico riconoscimento del diritto alla cancellazione dei dati dell'interessato. Il corretto inquadramento del problema presuppone dapprima una chiara individuazione del ruolo attribuibile a ciascun soggetto.

Il GDPR è chiarissimo nell'attribuire la responsabilità per la cancellazione dei dati al titolare del trattamento e, dunque, l'effettivo impatto del diritto all'oblio sui sistemi IoT deve misurarsi con l'individuazione di quest'ultimo. Né pare che la normativa attuale ammetta di prediligere gli interessi economici del titolare del trattamento a scapito della tutela dei dati personali. Piuttosto entra qui in gioco ancora una volta il problema di trovare un equilibrio che consenta di incoraggiare lo sviluppo della tecnologia e dell'innovazione, senza però sacrificare la tutela dei diritti fondamentali dell'individuo.

Il riconoscimento a livello legislativo del diritto all'oblio può essere per certi versi considerato come il punto di arrivo di un percorso giurisprudenziale e di evoluzione interpretativa finalizzato ad ampliare lo spettro di protezione dei diritti della personalità, che nel nostro ordinamento trovano pieno riconoscimento nell'art. 2 della Costituzione[302]. A livello europeo, ma anche e specularmente a livello nazionale, è stata accolta un'interpretazione dinamica di tali diritti, nella convinzione che questo sia l'unico approccio effettivamente in grado di garantirne la piena tutela, seppure nel contesto complesso e in continuo cambiamento determinato dalle nuove tecnologie.

L'impatto della sentenza *Google Spain* in relazione ai sistemi IoT va dunque inquadrato, più in generale, nell'ambito della questione relativa al rapporto fra il valore economico dei dati e la tutela dei diritti fondamentali dell'individuo. La sentenza, infatti, rappresenta uno degli step fondamentali nel processo di "costituzionalizzazione" del diritto alla protezione dei dati personali, e la sua rilevanza si coglie proprio nel fatto che la CGUE, pur riconoscendo l'esistenza di interessi economici dei motori di ricerca, ha comunque affermato la preminenza della tutela dell'individuo rispetto a questi ultimi[303].

Dando rilievo a questo aspetto, si comprende che garantire pieno riconoscimento ed effettività al diritto di cancellazione dei dati può costituire un enorme limite allo sviluppo e alla diffusione dei sistemi IoT e delle *smart city*. A fronte dell'opportunità di costruire un vero e proprio mercato dei dati, in cui gli stessi individui siano in grado di trarre vantaggio economico dall'utilizzo dei propri dati personali, non

[302] Sammarco (n. 189), 179-181. Interessante osservare il riferimento alla disciplina antitrust e al tacito riconoscimento della CGUE di una posizione "dominante" dei motori di ricerca in un contesto profondamente diverso da quello attuale. Se ne deduce che, sebbene la convergenza fra le due discipline sia stata solo recentemente e ancora non del tutto riconosciuta, vi è già da tempo una latente consapevolezza del sempre maggior potere che i nuovi attori hanno acquisito sul mercato.

[303] Vincenzo Ricciuto, "I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato", in Nadia Zorzi Galgano *Persona e Mercato Dei Dati: Riflessioni Sul GDPR*, (2019), vol. 175 (Milano, Padova, Wolters Kluwer), 95-96.

possono infatti essere trascurati gli enormi rischi in cui questi ultimi incorrono. A tal proposito basti richiamare quanto si è detto relativamente alla profilazione, nonché alle possibili discriminazioni.

Sotto questo profilo, l'insegnamento che lascia la sentenza *Google Spain* è la necessità di tenere a mente il valore che l'ordinamento europeo riconosce alla tutela dei dati personali, elevata a rango di diritto fondamentale dalla Carta di Nizza, da cui deriva il divieto di sacrificare la tutela in nome degli interessi economici, principio che può senz'altro affermarsi anche con riferimento ai sistemi IoT.

Un'apertura verso la diffusione dei sistemi IoT e lo sviluppo delle *smart city* potrebbe comunque aversi contemperando il diritto alla tutela dei dati personali con il perseguimento dell'interesse generale a favorire il progresso e l'innovazione. Si ricordi, infatti, che il diritto in esame non è concepito dal GDPR come un diritto assoluto, ma da bilanciare rispetto agli altri interessi che vengono in rilievo[304]. Sebbene fino ad ora il dibattito si sia incentrato soprattutto sul rapporto fra diritto alla cancellazione e libertà di informazione, non è da escludersi che un bilanciamento di interessi possa essere effettuato anche con riferimento allo sviluppo ed all'innovazione, al centro del dibattito politico ed istituzionale a livello europeo e non solo.

C. La DPIA

Si è già detto che la DPIA[305] è uno strumento fondamentale di cui può (e in alcuni casi deve) servirsi il titolare del trattamento nella fase di valutazione preventiva dei rischi legati al trattamento dei dati personali al fine di garantire e dimostrare il rispetto della disciplina dettata dal GDPR. Fra le ipotesi in cui la DPIA dev'essere obbligatoriamente disposta ve ne sono alcune senz'altro rilevanti in riferimento ai sistemi IoT. Questo è il caso, ad esempio, di trattamenti che prevedano la valutazione sistematica di profili personali delle persone fisiche, basata su processi automatizzati, ivi inclusa la profilazione. Più in generale, l'obbligo di disporre la DPIA sussiste anche nel caso in cui siano utilizzate nuove tecnologie e questo possa tradursi in un grave rischio per i diritti e le libertà delle persone. Le linee-guida disposte dall'Art. 29 WP sulla DPIA[306] prevedono che, al fine di garantire il massimo rispetto del principio di trasparenza e porre il soggetto interessato nelle condizioni di prestare il proprio consenso in modo informato e consapevole, i risultati della DPIA vengano resi (almeno parzialmente) pubblici e siano soggetti a controllo ed aggiornamento periodici. Sebbene le suddette linee-guida non abbiano carattere obbligatorio, l'osservanza di tali disposizioni contribuirebbe senz'altro ad accrescere i livelli di fiducia che gli utenti ripongono nei dispositivi IoT, favorendone la diffusione e l'utilizzo[307]. È bene qui ribadire ancora una volta che, proprio in ragione del ruolo determinante della fiducia degli utenti nel futuro delle

[304] Si veda Capitolo I, p. 57.
[305] Si veda Capitolo I, pag. 52.
[306] Art. 29 WP, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", accessibile da https://ec.europa.eu/newsroom/document.cfm?doc_id=47711.
[307] Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model" (n. 239), 278.

nuove tecnologie, anche nel caso in cui non sussistessero le condizioni necessarie perché vi sia l'obbligo di predisporre la DPIA, gli sviluppatori dei sistemi IoT dovrebbero tenere conto dei rischi a cui gli individui sono esposti già in fase di progettazione, studiando soluzioni tecniche volte a ridurne l'impatto.

D. Il titolare e il responsabile del trattamento

A questo punto bisogna affrontare il discorso più volte richiamato sull'individuazione del titolare del trattamento nell'ambito dei sistemi IoT. Come già detto, questo è responsabile per la determinazione dei mezzi e delle finalità del trattamento, ma anche del rispetto dei principi generali e dei diritti dell'interessato[308].

L'individuazione del titolare e del responsabile del trattamento dovrà avvenire adottando un'interpretazione funzionale di questi ruoli e cioè guardando al ruolo effettivamente svolto dai singoli soggetti. In questo modo si avrà una corretta allocazione della responsabilità, basata sulla capacità di controllo che ciascun soggetto ha concretamente sul trattamento[309]. Ciò è tanto più vero nel caso di sistemi complessi come gli IoT, il cui funzionamento implica l'intervento attivo di svariati soggetti a cui può essere riconosciuto un grado di responsabilità diverso in relazione alle singole fasi e funzioni svolte[310].

In primo luogo devono essere chiamati in causa i **produttori**, responsabili non soltanto della vendita dei prodotti, ma soprattutto della loro progettazione e creazione, attività che include fra le altre cose l'inserimento all'interno dei dispositivi dei sensori e delle altre tecnologie che consentono primariamente la raccolta dei dati. Sono i produttori a decidere quali dati saranno raccolti, con quale frequenza e a quale scopo. Per tale ragione dovrebbero ricadere senza dubbio nella definizione di titolari del trattamento ai sensi del GDPR.

La disciplina attuale non è tuttavia chiara sul punto, non menzionando esplicitamente i produttori fra i soggetti tenuti al rispetto degli obblighi in materia di tutela dei dati. Sarebbe opportuno dettare una disciplina più dettagliata, che imponga di tenere i considerazione i problemi relativi alla tutela dei dati già in fase di progettazione, facendo ricadere espressamente la responsabilità per la violazione delle norme sui soggetti coinvolti in questa fase[311]. Un intervento limitato alla sola fase contrattuale, con la

[308] GDPR, art. 24; FRA, ECHR, CoE, (n. 135), 101-103. Nel caso in cui più soggetti siano chiamati a definire congiuntamente i mezzi e le finalità, si avrà la figura del co-titolare. Il titolare dovrà essere in grado di dimostrare alle autorità competenti di aver disposto tutte le misure possibili e adeguate a prevenire eventuali *data breach*, avendo comunque l'obbligo di notificare immediatamente l'ipotesi in cui si verifichino. Al titolare del trattamento viene riconosciuto il diritto di nominare il responsabile del trattamento, chiamato a svolgere alcune funzioni in nome e per conto del titolare, ad esempio predisponendo la DPIA o preoccupandosi di notificare alle autorità. Individuare con certezza chi possa essere identificato come titolare del trattamento è presupposto imprescindibile per garantire il pieno rispetto della disciplina dettata dal GDPR, in primo luogo perché è su di lui che ricade l'eventuale responsabilità per le violazioni subite dal soggetto interessato, ma anche perché è proprio al titolare che l'interessato può rivolgersi per ottenere chiarimenti sul trattamento o sollevare contestazioni.

[309] EDPB, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", 9.

[310] Art 29 WP, "Opinion 8/2014 on the on Recent Developments on the Internet of Things" (n. 239), 11-13.

[311] Pappagallo, Durante, Monteleone (n. 128), 71-72.

disposizione di obblighi legali in capo alle parti, sarebbe insufficiente a garantire il rispetto effettivo della disciplina, tenuto conto della struttura e delle caratteristiche intrinseche ai sistemi IoT. Inoltre è possibile che i dati generati e condivisi dagli utenti siano ulteriormente condivisi attraverso i *social network*, spesso sulla base di meccanismi automatici definiti dalle opzioni di default[312]. Ciò comporta il trattamento dei dati per fini diversi e ulteriori e, oltre a porre dei problemi in termini di validità del consenso prestato e di rispetto dei principi summenzionati, fa sì che le piattaforme social acquisiscano il ruolo di titolari del trattamento per i dati con esse condivisi. Il livello di interfaccia con l'utente prevede poi spesso l'utilizzo di API, che consentono la connessione con *app* gestite da terze parti, circostanza che presuppone che l'utente presti il proprio consenso in modo libero, specifico e informato. Tralasciando i problemi già analizzati sotto questo profilo, se i dati vengono condivisi con tali soggetti, graveranno su questi ultimi gli obblighi dettati dal GDPR. Infine, i dati potrebbero essere ceduti ad altri terzi che hanno interesse ad elaborarli per fini ulteriori. Si fa l'esempio di società assicurative che utilizzano i dati per il calcolo dei premi. Sebbene a differenza dei produttori e degli sviluppatori di *app* questi non abbiano un effettivo controllo sui dati raccolti, saranno comunque qualificabili come titolari del trattamento, dal momento che raccolgono e trattano dati per fini che loro stessi hanno individuato. Infine, il problema di interoperabilità dei dati ha portato allo sviluppo di piattaforme che consentono di raccogliere dati generati da dispositivi diversi, con un sistema di gestione centralizzata e semplificata.

Tali piattaforme acquisiranno lo status di titolare del trattamento nella misura in cui sviluppino servizi basati sul trattamento di dati per quale individuano specificatamente le finalità. Gli utenti che si interfacciano con i dispositivi IoT sarebbero invece qualificati come responsabili del trattamento[313].

Queste disposizioni sembrano però porsi in contrasto con l'approccio adottato dallo stesso Art. 29 WP rispetto ai sistemi di *cloud computing*[314]. In tal caso, infatti, la qualifica di titolare del trattamento sarebbe spettata al cliente del servizio. L'incoerenza che emerge dal quadro generale della disciplina è particolarmente problematica se si pensa che i sistemi IoT sfruttano generalmente architetture *cloud* per la gestione dei propri dati. Ne deriverebbe infatti un'ingiustificata e pericolosa confusione nell'attribuzione dei ruoli ai vari soggetti coinvolti. La soluzione va ricercata richiamando quell'approccio funzionale nella definizione dei ruoli a cui si è fatto riferimento in precedenza. L'attribuzione della qualità di titolare del trattamento ai clienti dei sistemi *cloud* era stata giustificata sulla base della considerazione che è proprio il cliente a decidere sull'assegnazione di parte o della

[312] Art 29 WP, "Opinion 8/2014 on the on Recent Developments on the Internet of Things" (n. 239), 12.
[313] Si noti che parte della dottrina critica a monte la distinzione fra attori diversi nel contesto del trattamento dei dati personali, ed in particolare della distinzione fra titolare e responsabile del trattamento, reputandola inadatta ai nuovi contesti e ai più recenti sviluppi della tecnologia. La figura del responsabile viene infatti descritta come una possibile via di fuga per soggetti che, pur coinvolti nel trattamento dei dati, sarebbero gravati da minore responsabilità di fronte alla legge. Si veda in generale Paul de Hert, Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?", 2016, vol. 32/no. 2, The Computer Law and Security Report, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364916300346?via%3Dihub.
[314] Mantelero, Vaciago (n. 137), 567.

totalità del trattamento dei servizi *cloud* per sistemi specifici. Tale argomento può essere richiamato anche nel contesto dei sistemi IoT, dovendo però distinguere fra le diverse categorie di dati trattati. Come si è visto parlando del diritto alla portabilità dei dati, infatti, questi ultimi possono essere diversamente qualificati a seconda che siano forniti volontariamente dall'interessato, generati nel corso dell'utilizzo del dispositivo o, infine, dedotti o predetti mediante l'uso di sistemi di analisi. Quanto alla prima tipologia di dati, ossia quelli volontariamente forniti dall'interessato, gli utenti che usufruiscono del sistema IoT (utilizzatori) potrebbero allora essere qualificati come titolare, mentre per le altre categorie produttore e utilizzatore dovrebbero figurare come co-titolari. Seguire l'una o l'altra interpretazione avrà chiaramente delle conseguenze in termini di possibilità per l'interessato di esercitare concretamente i propri diritti.

Il discorso si complica ancor di più alla luce delle possibili integrazioni fra i sistemi IoT e le altre tecnologie, prima fra tutte l'AI. È già possibile, anche se nel futuro prossimo ci si aspetta un livello di diffusione certamente maggiore, pensare a dispositivi autonomi che siano in grado di interagire con l'ambiente circostante e assumere decisioni. Chi può essere considerato come responsabile del trattamento in questa ipotesi? Secondo un progetto risalente al 2014, chiamato "Robot Law" [315], l'utente doveva essere legalmente obbligato ad adottare misure di sicurezza idonee a preservare i dati personali durante l'utilizzo dei dispositivi. La tesi si basava sulla considerazione che è l'utente – e non ad esempio il produttore – il vero detentore dei dati, e che da ciò ne conseguisse che gli obblighi derivanti dal rispetto della disciplina sulla tutela dei dati personali gravassero proprio su quest'ultimo. Questa posizione non è però convincente, specialmente sulla base del fatto che le prime applicazioni dei dispositivi in esame hanno dimostrato che il trattamento illecito dei dati è nella maggior parte dei casi la conseguenza di difetti o errori di progettazione attribuibili ai produttori.

Richiamando l'approccio funzionale alla nozione di titolare del trattamento di cui sopra, bisognerebbe individuare il soggetto in grado di esercitare un controllo effettivo su tali dispositivi. Rilevante in tal senso è il dibattito concernente i sistemi AI, rispetto ai quali si discute sulla possibilità o meno di attribuire loro personalità giuridica[316]. Se l'esito del dibattito fosse positivo, probabilmente la risposta all'interrogativo sulla concreta individuazione del titolare del trattamento sarebbe più semplice, coincidendo quest'ultimo con il sistema stesso. I più recenti sviluppi a livello europeo in materia di responsabilità civile nei sistemi AI sembrano però condurre verso una direzione diversa.

Nella proposta di Regolamento elaborata dalla Commissione nell'aprile 2021[317] si propende per l'adozione di un regime che allochi la responsabilità civile in capo ai cosiddetti "provider", pur

[315] Pappagallo, Durante, Monteleone (n. 128), 72-73.
[316] Butterworth, (n. 166), 261.
[317] Commission, "Proposal of 21 April 2021 for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM(2021) 206 final, accessibile da https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75788.

distinguendo a seconda del livello di rischio riconosciuto a ciascun sistema. Il discorso è rilevante anche ai fini dell'applicazione della disciplina sulla tutela dei dati per diversi motivi. In primo luogo, nell'elaborare tale proposta è stato adottato un approccio che ricalca la ratio del GDPR, specie per quanto riguarda le modalità di determinazione del rischio[318]. Inoltre, la Proposta di Regolamento prevede che lo stesso produttore possa assumere la qualifica di provider in determinate circostanze[319]. Nel quadro di un'evoluzione normativa coerente ed omogenea a livello europeo, è chiaro dunque che la direzione che si deciderà di intraprendere in un settore inevitabilmente influenzerà anche lo sviluppo dell'altro.

2.1.3 Internet of things, algoritmi e diritto alla concorrenza: i limiti e le potenzialità della disciplina europea di fronte alle nuove tecnologie

Si è già detto che lo sviluppo delle nuove tecnologie e il fenomeno dei Big Data hanno fatto emergere nuovi modelli di *business*, influenzando il rapporto fra le imprese concorrenti sul mercato. Si è inoltre detto che, di fronte a queste novità, la disciplina dell'UE sulla concorrenza attualmente vigente ha mostrato i propri limiti, inducendo le autorità competenti e alcuni legislatori a livello nazionale ad esplorare soluzioni nuove in grado di rispondere meglio alle nuove esigenze.

A questo punto è bene affrontare il discorso in maniera più sistematica, analizzando più da vicino le sfide che lo sviluppo di sistemi IoT e l'impiego di tecniche di analisi dei dati pongono in termini di salvaguardia della libera concorrenza sul mercato.

A. Il mercato rilevante

Il mercato del prodotto

Come già messo in luce nel corso del capitolo I, al fine di adeguare la disciplina vigente ai cambiamenti portati sul mercato dall'emergere delle nuove tecnologie, il legislatore UE dovrebbe intervenire in prima istanza sulla definizione di mercato rilevante. Proprio in virtù del continuo e massiccio scambio di dati fra i dispositivi che costituiscono i sistemi IoT, nonché della possibilità che tali dati siano condivisi con soggetti terzi, è ben possibile che un'impresa operante su un determinato mercato acquisisca informazioni tali da riuscire facilmente ad ampliare la propria attività anche su un mercato adiacente. Per fornire un esempio pratico di quanto qui si sta discutendo, si pensi al mercato automobilistico e alla sua integrazione con quello assicurativo[320]. L'*automotive* è infatti uno dei settori in cui l'impiego di sistemi IoT è già maggiormente diffuso e promette di divenire ancora più determinante nel prossimo futuro. Grazie a sensori e videocamere, le automobili sono ad oggi in grado di rilevare lo stile di guida del conducente, comunicare con il GPS per individuare il percorso migliore e via discorrendo. Si pensi

[318] Policy Department for Citizens' rights and constitutional affairs, "Artificial intelligence and civil liability".
[319] Nello specifico, il produttore risponderà dei danni provocati dal sistema AI nell'ipotesi in cui questo stesso sia il prodotto oppure una sua componente di sicurezza.
[320] AGCM, AGCOM, GPDP, (n. 8), 80.

all'impatto che potrebbe avere la collaborazione e lo scambio di dati fra le società automobilistiche e i servizi assicurativi, in grado di differenziare i premi delle polizze secondo le peculiarità di ciascun cliente. In questo caso, costruire un sistema che garantisca maggiore trasparenza sui dati che vengono scambiati e i soggetti che beneficiano di tali scambi, avrebbe un impatto positivo non soltanto sul piano della tutela dei dati personali, ma anche su quello concorrenziale. In questo senso si comprendono le ragioni sottostanti le nuove misure e i nuovi obblighi che sarebbero posti in capo ai cosiddetti *gatekeeper* alla luce del Digital Market Act e del Digital Service Act[321].

Si consideri inoltre che il discorso relativo alla capacità delle imprese di estendersi su mercati ulteriori rispetto a quello nel quale operano in via principale o addirittura inesistenti nel momento in cui intraprendono la propria attività vale a maggior ragione nel campo dell'intelligenza artificiale, di cui si è ampiamente illustrato lo stretto legame con i sistemi IoT[322]. Il rischio è dunque che si generino mercati in cui concorrano soltanto pochissime società, senza alcuna possibilità per le concorrenti di entrarne a far parte.

Il mercato geografico

Quanto al mercato geografico rilevante, occorrerà procedere ad un'analisi caso per caso, finalizzata ad indagare se effettivamente possa farsi una distinzione su base territoriale[323]. Occorrerà infatti verificare dove si trovano i singoli dispositivi che compongono il sistema e quale sia l'estensione geografica dell'attività svolta dagli stessi. Se in alcuni casi è possibile limitare tale attività ad una determinata area nazionale o regionale, in altri questo tipo di distinzione è non solo difficile, ma anche potenzialmente pericolosa. Non sempre, infatti, è facile stabilire con certezza e a priori dove avverrà di fatto l'erogazione di beni e servizi, né chi beneficerà dello scambio di dati. Limitare le indagini preordinate all'applicazione della disciplina concorrenziale ad un'area geografica definita e parziale potrebbe dunque comprometterne l'efficacia e l'effettività.

B. Il potere di mercato

Posto che i dati debbano essere ormai pacificamente riconosciuti quale *asset* strategico nella definizione del potere di mercato, trattando nello specifico del caso dei sistemi IoT, a concorrere alla determinazione di tale potere saranno non soltanto i dati generati e condivisi fra i dispositivi che compongono il sistema, ma anche (e soprattutto) gli algoritmi sviluppati per la loro analisi. Ancora una volta è bene qui ricordare che il valore economico dei dati dipende infatti dalle informazioni che è possibile trarne, variando sia in ragione della tipologia di dati che delle tecniche di analisi degli stessi.

[321] Vedi note 2 e 3.
[322] Maggiolino (n. 33), 321.
[323] Moritz, (n. 46), 366.

La proprietà dei dati

Tale discorso si ricollega naturalmente a quello relativo alla proprietà sui dati. L'assenza di una disciplina specifica in tal senso e le conseguenti difficoltà nell'allocazione dei diritti ad essa ricollegati, rende senz'altro più complesso definire chiaramente quale sia il potere di mercato di ciascun concorrente in relazione ai dati di cui ha la disponibilità. In altre parole, il valore economico dei dati – ed in particolare dei dati personali – porta a chiedersi se sia necessario ed opportuno introdurre un diritto reale di proprietà sui dati, da tenersi distinto rispetto ai diritti di proprietà intellettuale ed ai diritti che il GDPR riconosce all'interessato sui dati personali, introducendo una disciplina organica che consenta di determinare con certezza chi e a quali condizioni possa disporre liberamente dei dati e abbia diritto di godere dei benefici economici derivanti dal loro utilizzo[324]. Il discorso assume naturalmente rilevanza nel contesto dei sistemi IoT, le cui prestazioni sono imprescindibilmente legate al trattamento dei dati.

Nel dibattito sulla possibilità o meno di attribuire un diritto di proprietà assoluto sui dati personali, parte della dottrina[325] ritiene che debba essere fatta una distinzione fra dati intrinsecamente personali e dati solo estrinsecamente tali. Nella prima categoria vi rientrano ad esempio i dati biometrici o il DNA. Avere controllo su queste tipologie di dati viene equiparato ad avere un controllo di fatto sulla persona. In tal caso la configurabilità di un diritto di proprietà da parte di terzi (ad esempio, titolari del trattamento) andrebbe allora esclusa a priori, dal momento che ne discenderebbe un indebito potere sulla persona, a cui si ricollegano anche problemi di natura etica. Discorso diverso vale invece per la seconda categoria di dati, rispetto alla quale un diritto di proprietà da parte di terzi sarebbe, almeno in teoria, configurabile, e il dibattito si sposta piuttosto sull'origine di tale diritto, che può essere diversamente ricostruita a seconda che si prediliga un approccio positivistico oppure giusnaturalistico[326]. La scelta dell'uno o dell'altro ha delle conseguenze pratiche importanti e rilevanti anche nel contesto specifico dei sistemi IoT.

---

[324] Bisogna preliminarmente chiarire che il concetto di proprietà non è unitariamente definito all'interno dell'UE e vi sono delle notevoli differenze fra il modo in cui questo è concepito dagli ordinamenti di *civil law* e di *common law*. Per superare i problemi posti da queste differenze, al concetto di proprietà sui dati vengono generalmente ricondotti tutti i diritti reali esercitabili su di essi. Adottando un approccio forse più coerente alle caratteristiche dei dati, si preferisce di solito parlare piuttosto di controllo sui dati, utilizzando tale espressione sia con riferimento ai poteri che la persona fisica o giuridica che si trova nella disponibilità dei dati è in grado di esercitare su di essi, sia ai diritti che questa può concedere a terzi. (Janeček Václav, "Ownership of Personal Data in the Internet of Things", (2018), vol. 34, no. 5 The Computer Law and Security Report, 1041, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364918300487?via%3Dihub; Arthur Van der Wees, Janneke Breeuwsma e Andrea van Sleen, "IoT Societal Impact – Legal Considerations and Perspectives" in Dr. Ovidiu Vermesan, Dr. Peter Friess *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, (2016, River Publishers), 228accessibile da https://digital-strategy.ec.europa.eu/en/library/digitising-industry-internet-things-connecting-physical-digital-and-virtual-worlds).

[325] Václav, (n. 324), 1043.

[326] Nella concezione positivista del diritto, il diritto di proprietà discende da un'imposizione legislativa ed è proprio in virtù della legge che acquista rilevanza giuridica. Si tratta dunque di un diritto concesso, plasticamente raffigurabile con una linea che si muove dall'alto verso il basso. Al contrario, la dottrina giusnaturalista esclude che il diritto di proprietà sul bene sia concesso in forza di legge, sostenendo piuttosto che spetti naturalmente a chi si trova ad esercitare un potere *de facto* sul bene. In questo caso la rappresentazione plastica è dunque opposta, ossia quella di una linea che si muove dal basso verso l'alto.

I fautori della tesi giusnaturalista ritengono che un diritto di proprietà assoluta sui dati personali possa essere riconosciuto solo al soggetto interessato, portando a sostegno della propria tesi argomenti sia di natura economica che legale[327]. Sotto questo secondo profilo, l'argomento principale richiama il diritto naturale di ciascun individuo di avere pieno controllo sui propri dati personali. Concetto che tra l'altro sottende alla *ratio* della disciplina del GDPR. Dal punto di vista economico, invece, si ritiene che attribuendo il controllo sui dati agli utenti piuttosto che alle piattaforme o ad altre strutture centralizzate responsabili della loro gestione, si avrebbero effetti positivi sulla concorrenza, riconducibili anche al rafforzamento del diritto alla portabilità dei dati.

Riconoscere agli utenti e non alle piattaforme il potere di disposizione sui dati vuol dire infatti privare queste ultime di uno dei fattori principali nell'acquisizione di potere di mercato e nella creazione di posizioni dominanti. Sono gli utenti a decidere a chi cedere i propri dati, sulla base della qualità del servizio o del prodotto offerto. Questo favorirebbe le imprese più piccole, che avrebbero così uguale accesso alle risorse, incoraggiando al contempo il miglioramento dei servizi e dei prodotti offerti.

Contro questa tesi si argomenta generalmente che la struttura stessa dei sistemi IoT renderebbe tecnicamente impossibile attribuire agli utenti un pieno controllo sui propri dati personali, in violazione del generale principio di inalienabilità dei diritti fondamentali. I dati generati all'interno dei sistemi IoT vengono infatti continuamente copiati, condivisi e trasmessi fra i vari dispositivi, in modo così rilevante che sarebbe illusorio pensare che il singolo utente possa mantenere su di essi un controllo effettivo. Allo stesso tempo, però, riconoscere il diritto di proprietà sui dati ad un sistema organizzato in maniera centralizzata, privando gli utenti di un controllo su di essi, non è certamente una soluzione coerente alla disciplina dell'UE, né allo status di diritto fondamentale riconosciuto alla protezione dei dati personali.

Per uscire dall'impasse occorrerebbe piuttosto intervenire sul piano tecnico, studiando un meccanismo trasparente che consenta all'interessato di controllare chi ha accesso ai propri dati e quale utilizzo ne viene fatto. In questi termini, l'integrazione con la tecnologia *blockchain* e l'introduzione di un sistema di *smart contract* che regoli i diritti di accesso ai dati potrebbe rappresentare una soluzione tanto innovativa quanto efficace.

Un altro limite dell'approccio naturalistico è dato dal fatto che questa teoria attribuisce valore ai dati in quanto tali, senza tenere in considerazione gli investimenti fatti dalle imprese per sviluppare ed utilizzare i sistemi di analisi che consentono di sfruttarli commercialmente. Si può infatti sostenere che proprio dall'attività di analisi ed elaborazione dei dati discenda in capo alle imprese un diritto di proprietà su di essi.

[327] Václav, (n. 324), 1044-45.

Approccio che risulta coerente sia con quanto stabilito dal GDPR in merito al diritto sulla portabilità dei dati, la cui applicazione è limitata ai soli dati forniti dall'interessato (e non anche ai cosiddetti dati inferenziali, protetti invece dalla disciplina sulla proprietà intellettuale), sia con l'indirizzo adottato dalla Commissione, favorevole a riconoscere diritti sui dati ai soggetti che riescono a trarne valore economico. Un conto, però, è parlare di diritti di proprietà intellettuale, un altro riconoscere un diritto di proprietà assoluto. Il riconoscimento di tale diritto ad un ente centralizzato, e non all'individuo a cui i dati sono riferibili, risulterebbe arbitrario e ingiustificato alla luce della natura di diritti fondamentali riconosciuta tanto al diritto di proprietà, quanto a quello di tutela dei dati personali, oltre al fatto che la competenza a legiferare sul diritto di proprietà è esclusa da quelle attribuite all'Unione Europea e spetta ai singoli Stati Membri[328].

Propendere per un approccio giusnaturalista solleva anche problemi di natura etica, dovendosi tenere conto del fatto che gli individui sarebbero esposti al rischio di pratiche commerciali scorrette o possibili discriminazioni[329]. Specie nel contesto dei sistemi IoT in cui - è sempre bene ribadirlo - la condivisione e la trasmissione dei dati è continua e può avvenire anche fra dispositivi collocati in aree geografiche diverse, l'elaborazione di una nuova disciplina che garantisca la tutela dei diritti fondamentali – tanto quello di proprietà, quanto quello di tutela dei dati – dovrebbe necessariamente accompagnarsi a nuove soluzioni anche dal punto di vista tecnico. Un tema sempre ricorrente è quello della trasparenza, relativa soprattutto all'utilizzo che viene fatto dei dati e al conseguente valore economico che questi assumono. Anche in questo senso, la creazione di un sistema di gestione dei dati basato su regole chiare, predeterminate e condivise, attraverso l'utilizzo degli *smart contract*, si sposerebbe bene con la necessità di garantire un'applicazione effettiva della disciplina.

C. Art. 101 TFUE

Si è già detto che l'art. 101 TFUE vieta gli accordi fra imprese, le decisioni fra associazioni di imprese e tutte le pratiche concordate che possano pregiudicare il commercio tra Stati Membri e che abbiano per oggetto o per effetto di impedire, restringere o falsare il gioco della concorrenza all'interno del mercato interno, sanzionando con la nullità ogni atto che rientri in una di queste attività[330].

Il primo comma elenca anche una serie di comportamenti che si considerano generalmente rilevanti per l'applicazione della norma, sebbene non si tratti di un elenco esaustivo. Il terzo comma individua invece deroghe, elencando le condizioni necessarie affinché la sanzione prevista dall'articolo in esame non operi.

[328] Ibid, 1049-50.
[329] Ibid, 1051.
[330] Whish, Bailey (n. 22), 82-83.

Art.101(1) TFUE – le pratiche concordate

Nel corso del capitolo I si è già avuto modo di analizzare i problemi che discendono dall'applicazione dell'art. 101(1) TFUE alle pratiche commerciali poste in essere dagli algoritmi, laddove l'intervento e la volontà umane sono limitate se non addirittura assenti. Nonostante le difficoltà nell'indagare questi comportamenti, vi sono alcuni elementi che possono guidare e aiutare nella valutazione[331]. In primo luogo il rischio di comportamenti collusivi sarà tanto maggiore nei mercati caratterizzati da una forte asimmetria informativa fra i concorrenti. La soluzione potrebbe essere quella di limitare l'accesso ai dati o almeno ad alcune categorie di questi, ma nel caso dei sistemi IoT questo potrebbe avvenire soltanto mediante l'introduzione di soluzioni di natura tecnica prima che normativa. La regolamentazione dei permessi di accesso ai dati in via automatizzata mediante *smart contact* potrebbe contribuire ad arginare questo problema. In ogni caso, i futuri interventi non potranno prescindere da una rivalutazione del rapporto fra macchine e uomo[332]. È necessaria un'indagine precisa sul livello di controllo che gli agenti effettivamente hanno e del tipo di responsabilità loro attribuibile rispetto alle scelte assunte dagli algoritmi. Come visto, sarà forse necessario anticipare la valutazione ad una fase precedente, ossia quella di programmazione stessa.

Un'altra condotta particolare alla quale si assiste già nell'attività svolta dalle piattaforme e che potrebbe avere rilievo anche nello specifico contesto dei sistemi IoT, configurando anche in tal caso una violazione dell'art. 101 TFUE, è il cosiddetto *geopricing*. Con questo termine s'intende l'accordo fra produttore e distributori in virtù del quale il primo impone ai secondi la vendita dei prodotti a prezzi differenziati in base al Paese. La pratica è rilevante per la disciplina antitrust se rappresenta la conseguenza dell'accordo fra due parti, in quanto sussistono gli elementi costitutivi della norma in esame[333].

Art. 101(3) – Le esenzioni dall'applicazione della norma

Come già anticipato, il terzo comma dell'articolo individua alcune specifiche condizioni in presenza delle quali la sanzione prevista per far fronte ai fenomeni collusivi non trova applicazione. Accanto a questa disposizione è stato poi elaborato il Regolamento (CE) 1/2003. Delinea anch'esso le condizioni in presenza delle quali l'art. 101 TFUE non trova applicazione, ma si basa maggiormente su criteri dimensionali e quantitativi.

---

[331] Ariel Ezrachi e Manurice E. Stucke, "Artificial intelligence & collusion: when computers inhibit competition", (2017), no. 5 University of Illinois Law Review, 1799-1802, accessibile da https://heinonline.org/HOL/P?h=hein.journals/unilllr2017&i=1816,.
[332] Sidharth, (n. 46), 140.
[333] Roberto Visconti Moro, "Danno antitrust e piattaforme digitali", (2021), vol. 1 *Il Diritto industriale*, 11.

L'applicazione dell'art. 101(3) TFUE è subordinata all'esistenza di quattro condizioni cumulative e l'onere della prova cade sull'impresa che intende dimostrare la legittimità della propria condotta[334]. Qualunque tipo di accordo o pratica concordata è suscettibile, almeno in linea teorica, di ricadere entro l'ambito di applicazione del terzo comma, ivi comprese le restrizioni per oggetto e - per quello che qui maggiormente interessa - gli accordi aventi ad oggetto la determinazione dei prezzi e le restrizioni cosiddette verticali. Alcune delle condizioni necessarie all'applicazione del regime di deroga qui in esame sono particolarmente rilevanti nel caso dei sistemi IoT e potrebbero contribuire a garantirne uno sviluppo e una diffusione sostenibili rispetto alla vigente disciplina.

La prima condizione indicata dalla norma è che l'accordo o la pratica concordata determinino un miglioramento nella produzione o nella distribuzione dei prodotti o comunque contribuiscano al progresso tecnologico o economico[335]. Il miglioramento apportato andrà valutato in termini oggettivi e non può coincidere con un vantaggio specifico per l'impresa. La valutazione sarà fatta alla stregua degli effetti distorsivi che l'accordo provoca rispetto alla concorrenza in generale, dovendo essere proporzionato rispetto a quest'ultimo. Se si tratta di accordi i cui effetti si manifestano su più mercati, il vantaggio ad essi riconducibile andrà verificato in relazione a ciascuno di essi. Nel corso degli anni si sono contrapposte due diverse interpretazioni, una più restrittiva ed una più estensiva. Seguendo la prima interpretazione, avranno rilevanza esclusivamente i vantaggi di tipo economico riconducibili all'accordo. Di contro, l'interpretazione estensiva suggerisce di tenere in considerazione anche fattori ulteriori, facendo riferimento alle varie politiche portate avanti dall'UE, ad esempio nel settore industriale o per la tutela dell'ambiente. Ai dubbi sullo scopo effettivo della norma, sollevati dall'evoluzione giurisprudenziale, si contrappongono le linee-guida emanate dalla Commissione[336], che propende per un'interpretazione di tipo restrittivo, suggerendo che ai sensi dell'art. 101(3) TFUE abbiano rilevanza esclusivamente i vantaggi di tipo economico. Questi sono ricondotti a due diverse categorie, che tuttavia non è sempre semplice distinguere: efficienza dei costi ed efficienza qualitativa. La prima include lo sviluppo di tecniche e soluzioni innovative che consentono un risparmio sui costi sostenuti, mentre la seconda dà rilievo soprattutto agli accordi su ricerca e sviluppo.

Lo sviluppo di sistemi IoT e il miglioramento degli algoritmi utilizzati rappresentano senz'altro una forma di progresso tecnologico, che comporta un miglioramento dei prodotti forniti ai consumatori (anche in termini di personalizzazione degli stessi) e un vantaggio economico per le imprese. Qualche dubbio sulla possibilità di ritenere sussistente tale condizione potrebbe sorgere in relazione al fatto che la norma richieda un vantaggio oggettivo e generale, e non a beneficio della singola impresa. Vantaggio

[334] Whish, Bailey, (n. 22), 159-161.
[335] Ibid, 162-167.
[336] Commissione, "Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale" (Comunicazione) C 11/2, accessibile da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52011XC0114(04)&from=IT.

che potrebbe essere raggiunto, ad esempio, attraverso maggiori obblighi di trasparenza e condivisione dei dati. Anche in questo caso, l'integrazione con la *blockchain* potrebbe rappresentare uno strumento utile per raggiungere i suddetti obiettivi. Un'analisi costi-benefici sarà comunque necessaria per valutare questo genere di soluzioni siano in concreto attuabili e rispettino effettivamente la disciplina UE.

L'art. 101(3) lett. c) prevede quale altra condizione che i consumatori traggano equamente beneficio dai vantaggi che l'accordo o la pratica concordata in esame comportano[337]. Se vi sono più gruppi di consumatori coinvolti, i vantaggi andranno valutati per ciascuno di essi e gli effetti positivi nei loro confronti dovranno essere maggiori rispetto alle conseguenze negative. Anche in questo caso gli elementi di valutazione sono l'efficienza sui costi e quella sulla qualità e, per quanto riguarda la prima, la Commissione ha sottolineato che si dovrà tenere conto delle caratteristiche e della struttura del mercato, della natura e dell'importanza dei vantaggi che questa comporta, dell'elasticità della domanda e della portata delle restrizioni sulla concorrenza.

Queste prime due condizioni potrebbero giocare un ruolo importante nell'indagine sugli effetti distorsivi prodotti dagli algoritmi di prezzo. Non può infatti negarsi che, nonostante le possibili conseguenze negative, l'impiego di questi algoritmi determini anche maggiore trasparenza sul mercato ed una migliore allocazione delle risorse, da cui discende che i migliori beni e servizi siano disponibili al minor prezzo possibile[338]. Da un punto di vista statico, una migliore allocazione delle risorse comporta un incremento del benessere sociale, legato all'aumento della quantità dei beni scambiati[339]. Da un punto di vista dinamico, invece, la prospettiva di maggiori profitti per le imprese è un incentivo all'innovazione e allo sviluppo di soluzioni sempre migliori.

Alla luce di queste considerazioni, potrebbe argomentarsi che vi sia spazio perché nel caso dei sistemi IoT trovi applicazione almeno la prima delle due condizioni sopra illustrate. Premesso che tali vantaggi dovranno in ogni caso essere correlati agli effetti restrittivi sulla concorrenza, guardando alla seconda condizione sorgono dubbi ulteriori. La differenziazione dei prezzi derivante dall'utilizzo degli algoritmi potrebbe infatti comportare conseguenze diverse per diversi gruppi di consumatori, avendo un impatto positivo su alcuni, ma non su altri. Questo non si concilia con la costante interpretazione che è stata data della norma, secondo la quale, come si è già detto, tutti i gruppi di consumatori coinvolti devono egualmente trarre beneficio dall'accordo affinché il regime d'esenzione previsto trovi applicazione.

[337] Whish, Bailey, (n. 22) 170-172.
[338] Ezrachi, Stucke, (n. 331), 1781.
[339] AGCM, AGCOM, GPDP, (n. 8), 106 e Andrea Minuto Rizzo, "I profili antitrust del nuovo web e della nuova economia digitale", (2019), vol. 2 *Il Diritto Industriale*, 188.

La norma individua infine altre due condizioni: (i) che le restrizioni siano indispensabili per determinare i benefici in termini di miglioramento della produzione e per i consumatori e, (ii) che queste non incidano su una parte sostanziale del mercato interno[340].

La prima condizione sarà soddisfatta se non vi sono altre soluzioni economicamente convenienti che producono i medesimi vantaggi incidendo meno sulla concorrenza e se, al contempo, le restrizioni sono ragionevolmente necessarie al conseguimento dei suddetti vantaggi. Per valutare se sussista o meno la seconda condizione dovranno invece compararsi le condizioni del mercato prima e dopo l'accordo in esame, al fine di valutare quanto questo abbia inciso sul livello di concorrenza[341]. In entrambi i casi, sarà compito della Commissione, le autorità o le Corti nazionali – oltre all'accertamento da parte degli operatori economici che devono valutare se la pratica è in violazione o meno delle norme del Trattato - svolgere un'analisi caso per caso che tenga conto delle circostanze concrete, a maggior ragione in contesti innovativi ed inesplorati come quelli di cui qui si sta parlando.

D. Art. 102 TFUE

È stato già anticipato che l'art. 102 TFUE non vieta *per se* l'acquisizione di una posizione dominante, ma soltanto l'abuso di quest'ultima. Anzitutto, dovrà dunque procedersi ad un'analisi volta a determinare se l'impresa si trovi o meno in una posizione dominante, valutando solo successivamente il carattere eventualmente abusivo delle condotte. La norma elenca alcune condotte generalmente considerate abusive, anche se non si tratta di un elenco esaustivo, ma è onere delle Autorità competenti verificare di volta in volta se le condotte tenute da un'impresa dominante ricadano o meno entro l'ambito di applicazione dell'articolo.

L'esistenza di una posizione dominante

Diversi sono gli elementi che contribuiscono a determinare l'esistenza di una posizione dominante sul mercato, influendo sulla capacità dei concorrenti di entrare e/o permanere al suo interno. Si fa anzitutto riferimento alle barriere legali, ma anche ai vantaggi economici ed altri elementi fra cui l'innovazione tecnologica

a) Le barriere legali: la proprietà intellettuale.

Il rapporto fra la disciplina sulla proprietà intellettuale e i livelli di concorrenza sul mercato è di particolare interesse nel contesto dei sistemi IoT. Le due discipline – concorrenziale e IP – si pongono infatti in un rapporto di naturale tensione, determinato dal fatto che mentre la prima mira a favorire la libera concorrenza, mettendo a disposizione di tutti le medesime risorse, la seconda tende a proteggere

[340] Whish, Bailey (n. 22), 169.
[341] Ibid, 172.

le imprese, garantendo loro diritti esclusivi su beni immateriali, per incoraggiare l'innovazione e lo sviluppo[342]. Nel contesto dei sistemi IoT il legame fra le due discipline è importante per due ragioni. Da un lato, la disciplina sulla proprietà intellettuale, ed in particolare quella sui brevetti, potrebbe ostacolare lo sviluppo e la diffusione di tali sistemi. Dall'altro, come si è già avuto modo di vedere, il fatto che indagando sulle possibili violazioni della disciplina concorrenziale si sia fatto riferimento alle norme dettate in materia IP è stato uno degli argomenti a sostegno della tesi che intende attribuire alla disciplina sulla tutela dei dati personali la qualità di standard di valutazione.

Quanto al primo profilo, i problemi maggiori sono posti dai cosiddetti brevetti standard essenziali (*standard essential patents*, da qui in poi "SEPs")[343], che garantiscono l'interoperabilità fra dispositivi diversi. Senza l'accesso a questi standard il funzionamento dei sistemi IoT sarebbe semplicemente impossibile[344]. È chiaro dunque che le imprese che godono di diritti di proprietà intellettuale su di essi, si trovano in una posizione di netto vantaggio rispetto alle altre, ponendo seri rischi per la concorrenza. La differenza sostanziale rispetto a quanto avveniva nei mercati tradizionali è data dal fatto che in questo caso l'accesso agli standard dovrà essere garantito non soltanto alle imprese che operano nel medesimo mercato, ma anche a quelle provenienti da settori diversi. Si faccia l'esempio di una *smart home*, nella quale coopereranno fornitori di energia elettrica o gas o di servizi di riscaldamento.

Un abuso della posizione dominante dei possessori di questi standard, avrebbe dunque effetti devastanti sull'intero mercato.

Nell'analizzare la questione, la Commissione[345] ha posto ancora una volta l'accento sul fatto che non siano gli standard in sé a determinare un problema in termini di concorrenza, quanto la condotta in concreto tenuta dalle imprese e che, al fine di favorire uno sviluppo più sostenibile e sicuro di questi sistemi, dovrebbe preferirsi una soluzione che operi a monte, piuttosto che puntare all'irrogazione di sanzioni in virtù della disciplina concorrenziale o IP, che opererebbero comunque ex post. Interoperabilità, portabilità e risorse aperte sono dunque le parole chiave per il futuro dei sistemi IoT. Lo spazio d'intervento della disciplina concorrenziale consisterebbe nell'imporre ai detentori degli standard essenziali di condividere questi ultimi con i loro concorrenti, annullando il vantaggio competitivo che ne deriverebbe loro.

---

[342] Rupprecht Podszun, "Standard Essential Patents and Antitrust Law in the Age of Standardisation and the Internet of Things: Shifting Paradigms", (2019), vol. 50, no. 6, *IIC - International Review of Intellectual Property and Competition Law*, 2.

[343] Gli standard consentono infatti una rapida e facile diffusione e condivisione di informazioni fra diversi dispositivi, ma sono spesso basati su tecnologie brevettate. La concessione di licenze per il loro utilizzo è stata (e continua ad essere indispensabile) ad esempio nell'ambito delle telecomunicazioni ed è la stessa Commissione a riconoscere che giocherà un ruolo determinante nello sviluppo dei sistemi IoT (Commissione, "Communication from the Commission to the European Parliament, the Council and the European Economic And Social Committee Setting out the EU approach to Standard Essential Patents" (Communication), COM(2017) 712 final, accessibile da https://ec.europa.eu/docsroom/documents/26583/attachments/1/translations/en/renditions/native.

[344] Podszun, (n. 342), 8-11.

[345] Commissione europea, "Setting out the EU approach to Standard Essential Patent", (n. 343).

Una soluzione alla quale sembrano fare eco le nuove disposizioni del Digital Market Act[346] in relazione ai dati. La ratio che sottende ad entrambe, infatti, è quella di puntare alla condivisione delle risorse essenziali, eliminando alla base la fonte di potere sul mercato. Parlando di interoperabilità e condivisione, però, congiuntamente alle novità sul piano normativo, andrebbero introdotte nuove soluzioni anche sul piano tecnico e, anche in questo caso, l'integrazione dei sistemi IoT con un registro distribuito come la *blockchain*, che semplificherebbe la condivisione e lo scambio di dati e informazioni anche fra sistemi distinti, potrebbe rappresentare una valida soluzione.

b) Le barriere legali: la tutela dei dati personali

Sotto il secondo profilo, l'intersezione fra la disciplina concorrenziale e quella della tutela dei dati rileva anche nel senso che alcuni degli obblighi imposti dal GDPR potrebbero tradursi in ostacoli per le imprese più piccole, finendo con il rafforzare quelle già più forti sul mercato[347]. Si è già parlato del principio di *privacy-by-design* che impone al titolare del trattamento di individuare ed applicare le soluzioni tecniche ed organizzative in grado di garantire il miglior livello possibile di protezione dei dati personali. L'implementazione di queste soluzioni richiede il sostenimento di costi e l'impiego di risorse di cui le imprese dispongono in misura molto diversa le une dalle altre, con la conseguenza che quelle più piccole rischiano di essere spazzate fuori dal mercato. Il filone inaugurato dall'Autorità tedesca nel caso Facebook, in virtù del quale la disciplina sulla tutela dei dati personali diventa parametro di valutazione della disciplina antitrust, potrebbe aggravare questa situazione. Se da un lato è vero che il fine è quello di limitare la libertà delle imprese dominanti sul mercato, arginando i rischi per i consumatori in termini di deterioramento degli standard di protezione dei propri dati personali, dall'altro giungere ad ipotizzare l'adozione di meccanismi specifici e di sistemi di trasparenza e sicurezza particolarmente avanzati, tanto da parlare di *"trasparency by design"* o *"security by design"*[348] potrebbe rivelarsi un ostacolo all'entrata di nuove imprese sul mercato, specialmente di quelle più piccole e prive delle risorse, sia economiche che no, necessarie ad eguagliare questi standard di sicurezza. Il tema è spinoso, perché lo scopo è quello di garantire il giusto bilanciamento fra un'adeguata tutela dei consumatori e la possibilità per le imprese di operare liberamente sul mercato. Anche la garanzia del diritto alla portabilità dei dati, che pure è concepito quale uno dei diritti sanciti dal GDPR dal quale la concorrenza trarrebbe maggiori vantaggi, potrebbe comportare degli oneri eccessivi per le imprese più piccole, che si troverebbero in una posizione

[346] Vedi nota 2.
[347] Mauro Tommaso, "I Big Data tra protezione dei dati personali e diritto alla concorrenza" 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): Scritti in Memoria di Stefano Rodotà,* (n. 129), 668.
[348] Gambino, Manzi (n. 48), 334.

di svantaggio, potendo addirittura incorrere nel rischio di subire delle sanzioni laddove non fossero in grado di dare piena applicazione alla norma[349].

c) I vantaggi economici

Il secondo degli elementi che influiscono sull'esistenza di potenziali concorrenti è rappresentato dai vantaggi economici, categoria all'interno della quale rientrano diversi fattori[350]. In primo luogo, nel caso *United Brands Company e United Brands Continentaal BV contro Commissione delle Comunità europee* (C- 27/76) la CGUE vi ha incluso le cosiddette economie di scala, elemento che, come si è già avuto modo di vedere, è particolarmente rilevante nei mercati multilaterali su cui operano le piattaforme. Queste ultime, infatti, sono in grado di sfruttare le proprie infrastrutture abbattendo i costi fissi da sostenere per la creazione e l'aggiornamento dei *databases*, operando contestualmente su più fronti ed interfacciandosi con gruppi di utenti diversi[351]. Tale discorso vale allora a maggior ragione parlando di sistemi IoT. Un'impresa che integra tali sistemi nel proprio processo produttivo sarà infatti in grado di produrre, immagazzinare ed analizzare contestualmente una quantità sempre maggiore di dati, sfruttando la stessa infrastruttura. Il vantaggio competitivo che gliene deriva non dipenderà soltanto, come si è detto, dalla monetizzazione dei dati, ma anche dal fatto che proprio grazie all'infrastruttura di cui gode sarà in grado di accedere a tali risorse abbattendo i costi fissi che normalmente andrebbero sostenuti.

d) Altri fattori

Tra gli altri elementi qualificabili come veri e propri vantaggi economici e che sicuramente assumono particolare rilevanza nell'ambito dei sistemi IoT figurano poi il vantaggio tecnologico, l'accesso a specifiche risorse, gli investimenti nel settore di ricerca e sviluppo, ma anche le integrazioni verticali fra imprese[352].

Le condotte abusive

Il concetto di abuso ai sensi dell'art. 102 TFUE è inteso in senso oggettivo, per cui non rileva l'intenzione dell'impresa, ma soltanto le conseguenze concrete della sua attività sul mercato. In generale si possono

[349] Battelli, D'Ippolito Guido, (n. 190), 318.
[350] Whish, Bailey, (n. 22) 192.
[351] Haucap, (n. 18), 204.
[352] Whish, Bailey, (n. 22), 192-193.

distinguere due diverse categorie di abusi[353]: gli abusi di sfruttamento[354] e gli abusi di esclusione[355] e le forme di abuso che potrebbero avere luogo nel caso dei sistemi IoT rientrano nell'una e nell'altra categoria.

a) Gli abusi di sfruttamento

Nella prima categorie di condotte abusive rientra anzitutto il rifiuto a contrarre nei casi in cui i dati possono essere qualificati come *essential facilities*. La condotta è parimenti abusiva anche nel caso in cui l'accesso ai dati venga concesso in maniera discriminatoria o quando consegua alla stipulazione di contratti di esclusiva, che vincolano le imprese concorrenti[356]. Questo, ad esempio, è quanto la Commissione ha contestato a Google nel caso noto come *"Google Android"* risalente al 2019[357]. Alla pari, l'utilizzo incrociato dei dati, ossia l'utilizzo dei dati raccolti in un mercato per tentare di entrare o per rafforzare la propria posizione all'interno di un mercato diverso, potrebbe rappresentare un abuso di posizione. Rientrano nell'ambito di questa categoria anche le discriminazioni di prezzo che, come visto, queste possono senz'altro scaturire da forme di collusione fra le imprese, cadendo entro l'ambito di applicazione dell'art. 101 TFUE, o anche configurarsi come condotte individuali, aventi comunque effetti incisivi sulla concorrenza. Un'impresa in posizione dominante potrebbe ben scegliere di differenziare i prezzi di vendita dei propri prodotti sulla base dei dati che ha raccolto sui consumatori e al modo in cui questi sono stati categorizzati, fenomeno ancora più probabile nel caso di imprese che sfruttano i sistemi IoT, che accrescono notevolmente la mole di dati a loro disposizione. Sebbene si sia prima messo in luce che la differenziazione sui prezzi potrebbe avere anche effetti positivi sulla concorrenza, consentendo una migliore allocazione delle risorse e spronando le imprese a proporre

[353] Whish, Bailey, (n. 22), 207-216.

[354] Gli abusi di sfruttamento includono quelle forme di abuso caratterizzate dal fatto che l'impresa dominante sfrutti la propria posizione per ottenere maggiori guadagni a scapito dei propri clienti. Ad esempio, l'imposizione di clausole contrattuali inique o svantaggiose è generalmente qualificata proprio come un abuso di sfruttamento.

[355] Per abusi di esclusione s'intendono invece quelle condotte in grado di far uscire i concorrenti dal mercato oppure impedirne l'entrata. Possono essere sia verticali che orizzontali, a seconda che il concorrente escluso operi sullo stesso livello di mercato della dominante oppure in un mercato a valle. È ben possibile infatti che la condotta tenuta da un'impresa sul mercato principale determini effetti negativi per la concorrenza in un diverso mercato, ma non per questo potrà ritenersi esclusa dall'applicazione della norma in esame. A queste categoria vengono generalmente ricondotte diversi tipi di condotte, fra cui la discriminazione sui prezzi, il rifiuto di contrarre, il rifiuto di concedere la licenza per diritti di proprietà intellettuale o per consentire l'interoperabilità dei servizi.

[356] Autoritè de la concurrence e Bunderskartellamt, (n. 20), 18; AGCM, AGCOM, GPDP, (n. 8), 109-112.

[357] La società è stata infatti sanzionata per avere abusato della propria posizione dominante nel mercato dell'intermediazione pubblicitaria nei motori di ricerca. Attraverso la piattaforma AdSense for Search, Google opera come intermediario tra inserzionisti e proprietari di siti web. La condotta abusiva consisteva da un lato nell'avere imposto ai *publishers* dei contratti di fornitura esclusiva, in virtù dei quali a questi ultimi era preclusa la possibilità di inserire i propri annunci su altri siti web e, dall'altro, nell'avere implementato un sistema in grado sia di monitorare gli annunci dei concorrenti che di favorire i propri prodotti a scapito di quelli degli altri. Già nel 2017, Google era stata sanzionata dalla Commissione per avere abusato della propria posizione dominante nel mercato dei servizi di ricerca generica, in quanto l'algoritmo utilizzato dalla società tendeva a favorire nei risultati delle ricerche i prodotti di quest'ultima a scapito di quelli dei concorrenti. In tal caso era dunque proprio l'algoritmo utilizzato ad integrare la condotta escludente costituente l'abuso.

offerte più convenienti a quei consumatori che hanno manifestato maggiore interesse verso l'acquisto di un bene o servizio, per concorrere con le altre in modo effettivo, le possibili conseguenze negative riconducibili a questa pratica non sono poche, né di trascurabile importanza. La differenziazione dei prezzi potrebbe infatti determinare un incremento dei costi per la ricerca dei prodotti, nonché una riduzione del grado di sostituibilità degli stessi. Spetterà dunque alle Autorità competenti svolgere un'analisi concreta caso per caso, volta ad indagare l'effettiva sussistenza di profili di abusi e dovendosi invece escludere una condanna *tout court* della condotta. Soltanto tenuto conto degli effetti da questa prodotta sul mercato e in assenza di giustificazioni, la condotta tenuta dall'impresa dominante potrà infatti essere qualificata come abusiva.

Infine, il potere di un'impresa di ridurre il livello di protezione garantita sui dati personali o più in generale di modificare le condizioni contrattuali stabilite dalle *privacy policy*, oltre che un indice del potere di mercato detenuto, può costituire una vera e propria forma di abuso.

Un esempio in tal senso è dato sia dalla vicenda Facebook/WhatsApp[358], sia dalla più recente pronuncia Facebook Germany (B6-22/16)[359].

Nel primo caso la Commissione europea ha sanzionato Facebook proprio perché la società aveva modificato le condizioni contrattuali consentendo l'utilizzo incrociato dei dati raccolti attraverso le due piattaforme, peraltro contraddicendo le dichiarazioni rese nel corso delle indagini della Commissione in merito alla fusione fra le due.

Nel secondo caso invece il Bundeskartellamt tedesco ha stabilito che le condizioni di utilizzo dei dati trasmessi a Facebook da parte di terzi così come dettate dalla *privacy policy* integrassero condizioni contrattuali inique ai sensi dell'art. 102 TFUE. Più in generale, la raccolta eccessiva di dati attraverso soggetti terzi può integrare un abuso di posizione, facilitando la profilazione degli utenti e dunque rafforzando il potere di mercato delle imprese[360].

b) Gli abusi di esclusione

Nel caso dei sistemi IoT le condotte esclusive che potrebbero avere un maggiore impatto sulla concorrenza sono quelle attinenti alle limitazioni alla condivisione e circolazione dei dati. Il fatto che non tutte le imprese siano in grado di accedere agli stessi dati o comunque di trarne la stessa mole di informazioni, accresce il rischio che i limiti imposti alla loro circolazione comportino la creazione o il

[358] Facebook/Whatsapp (COMP/M 7217) Decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004 C(2014) 7239 final OJ C 297.
[359] Bundeskartellamt, (n. 1).
[360] Viktoria H. S. E. Robertson, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data" (2020), vol. 57, no. 1 Common Market Law Review, 162, accessibile da https://tinyurl.com/yfzqpls7.

rafforzamento di posizioni dominanti[361]. In questo senso alcuni dei principi stabiliti dal GDPR possono contribuire ad arginare il rischio di abusi.

Ad esempio, i principi di limitazione alla conservazione dei dati o di minimizzazione si pongono quale limite all'utilizzo indiscriminato dei dati da parte delle imprese. Ancora più rilevante per la concorrenza è poi il diritto alla portabilità dei dati, la cui vocazione economica è già stata ampiamente illustrata. Garantire all'interessato la possibilità di trasferire i propri dati personali ad un altro titolare senza dover sostenere costi aggiuntivi è una delle soluzioni che consente di evitare gli effetti dei cosiddetti *switching costs* e gli effetti *lock-in*, che determinano forti distorsioni della concorrenza. Il diritto in esame stimola la concorrenza anche perché le imprese saranno spronate ad offrire le migliori soluzioni per evitare che gli interessati scelgano di trasferire i propri dati ad un altro titolare. Va poi evidenziato che uno dei punti deboli del diritto alla portabilità dei dati è considerata la sua applicazione indiscriminata, ossia il fatto che i medesimi obblighi sono posti in capo a tutte le imprese, a prescindere dalla loro dimensione. Questo potrebbe infatti determinare un effetto opposto a quello sperato, distorcendo in maniera significativa la concorrenza[362]. L'applicazione della suddetta disciplina andrebbe allora subordinata alla preventiva determinazione che l'impresa titolare del trattamento si trovi in una posizione dominante, suggellando una strettissima relazione fra applicazione del diritto antitrust e della disciplina sulla tutela dei dati.

Chi si oppone a questa tesi basa le proprie argomentazioni sulla considerazione che il diritto alla portabilità dei dati rimane comunque un istituto tipico della disciplina del GDPR e che la sua applicabilità va quindi determinata esclusivamente alla stregua dei criteri propri di quest'ultima. In altre parole, viene ribadito ancora una volta che sebbene la convergenza fra le due discipline sia auspicabile, queste rimangono comunque distinte ed animate da ragioni e principi regolatori diversi.

Nel contesto del GDPR, il diritto alla portabilità dei dati mira a tutelare un diritto fondamentale e ciò ne giustifica l'applicabilità *ex ante*, a differenza di quanto avviene normalmente con le norme concorrenziali che invece individuano dei rimedi *ex post*. La strumentalità della portabilità dei dati alla tutela di un diritto fondamentale è inoltre la ragione giustificatrice della sua applicazione indistinta verso tutti i titolari del trattamento, a prescindere dalla loro dimensione o posizione di mercato. Questo non vuol dire che tali fattori non abbiano alcuna influenza sugli equilibri di mercato, ma soltanto che ad essi non è subordinata l'applicazione della disciplina sulla tutela dei dati, proprio per la diversa *ratio* e il diverso scopo da cui questa è ispirata. Una parte della dottrina ha sostenuto invece che il diritto alla portabilità possa essere configurato come una regola concorrenziale a priori. La violazione del diritto alla portabilità andrebbe dunque concepito automaticamente come una violazione della disciplina concorrenziale, senza indagare ulteriormente sugli effetti concreti che questo avrebbe sul mercato. Si è

[361] Tommaso, (n. 347), 669.
[362] Battelli, D'Ippolito (n. 190), 217-222.

fatto notare che, contrariamente a quanto si vorrebbe sostenere, questa impostazione rischia di ledere il dinamismo dei mercati digitali, incidendo negativamente sulla naturale "apertura" di queste economie. La vocazione economica del diritto alla portabilità dei dati e gli innegabili effetti che questo ha sugli equilibri di mercato forse sono però sufficienti a spiegare perché il legislatore europeo si sia ispirato proprio a questa disciplina nell'elaborazione della nuova regolamentazione sui mercati digitali.

Il Digital Market Act[363] attribuisce infatti alle imprese di dimensioni più piccole il diritto alla portabilità dei dati detenuti dai *gatekeeper*, al fine di indebolire il potere di mercato di questi ultimi e consentire ai primi di competere ad armi pari. Nonostante le critiche avanzate, concernenti soprattutto il fatto che i dati trasferiti dai *datasets* di provenienza rischiano di perdere almeno in parte il proprio valore economico, si coglie da un lato il cambio di rotta che il nuovo provvedimento promette di inaugurare, nel senso di una disciplina concorrenziale che sia in grado di intervenire in via preventiva e non soltanto rimediale e, dall'altro, la nuova consapevolezza da parte del legislatore europeo del legame esistente fra il controllo esercitato sui dati e la posizione di mercato. In ogni caso va tenuto conto del fatto che la nuova disciplina rimane comunque distinta rispetto a quella del GDPR, che continua a trovare applicazione con esclusivo riferimento al trattamento dei dati personali. Anzi, la nuova normativa dovrà essere comunque applicata nel rispetto della tutela dei dati personali. Inoltre, si badi bene, mentre le norme del Digital Market Act sono indirizzate alle imprese non dominanti, mentre per il GDPR è l'interessato il destinatario dei diritti ivi sanciti.

Si è più volte fatto presente che con la diffusione dei sistemi IoT, l'importanza di garantire portabilità dei dati, di pari passo con l'interoperabilità dei sistemi, crescerà sempre di più, poiché proprio a questi concetti è legato il loro corretto e miglior funzionamento. Da un punto di vista normativo, la strada è ancora in gran parte da definire, ma è ragionevole ritenere che questa dovrà necessariamente essere accompagnata da soluzioni tecniche che consentano di costruire dispositivi già strutturalmente compatibili con essa. Anche stavolta il richiamo è all'integrazione fra i sistemi IoT e la tecnologia *blockchain*, e al fatto che questo avvenga nell'ottica di uno sviluppo congiunto di tecnologia e legge.

2.2 Blockchain: il registro distribuito che ha stravolto il panorama della tecnologia.

2.2.1 Storia, funzionamento e applicazioni della blockchain

Si ritiene che la tecnologia *blockchain* sia stata introdotta per la prima volta da Satoshi Nakamoto nel 2009, con un *White Paper* nel quale venivano spiegate la struttura e le funzioni della criptovaluta

[363] Vedi nota 2.

Bitocoin[364]. Da quel momento il termine *blockchain* è stato ricollegato principalmente proprio al mondo delle criptovalute, sebbene le funzionalità che questa tecnologia può svolgere vadano ben oltre e trovino la propria origine in soluzioni elaborate già tempo prima della nascita di Bitcoin.

Le potenzialità mostrate dalla *blockchain* hanno indotto in poco tempo alla costruzione di nuove catene deputate allo svolgimento di attività totalmente diverse di quelle attinenti alle criptovalute, rilevanti sia nel settore pubblico che in quello privato. Nel settore privato le principali applicazioni riguardano la gestione di transazioni commerciali anche a livello nazionale o la creazione di piattaforme decentralizzate, nonché l'implementazione dei cosiddetti *smart contract*[365]. Nel settore pubblico, si pensa all'impiego di questa tecnologia per rafforzare i sistemi di sicurezza e contrastare più efficacemente gli attacchi informatici, al punto che l'UE sta studiando la possibilità di costruire una *blockchain* unica per tutto il territorio.

Come suggerisce il nome stesso, la *blockchain* può essere definita come una catena di blocchi collegati l'uno all'altro, in cui vengono registrati dati criptati mediante una funzione di *hash*[366]. Una volta che un blocco è completo, si procede alla creazione del blocco successivo, nel quale sarà anzitutto registrato il codice *hash* del blocco che lo precede. In questo modo non potranno esservi alterazioni dei dati registrati, poiché ogni alterazione comporterebbe una modifica del codice *hash* di tutti i blocchi. Sebbene tutti i blocchi siano egualmente coinvolti nella validazione delle transazioni, soltanto alcuni, definiti *miners*, saranno deputati alla creazione di nuovi blocchi[367]. Il funzionamento della catena si basa sul protocollo di consenso[368]. La sicurezza della catena è invece garantita dal fatto che non vi è un singolo *point of failure*, cioè un singolo punto suscettibile di attacchi. E' proprio la replicazione dei dati su più nodi che accresce il livello di sicurezza e resilienza della catena.

---

[364] Michèle Finck, "Blockchain technology" in *Blockchain Regulation and Governance in Europe*, (2019, Cambridge: Cambridge University Press,), 9, accessibile da https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04.

[365] Gli smart contract furono definiti per la prima volta da Szabo come "protocolli computerizzati che eseguono i termini di un contratto". Si tratta di contratti automatici, il cui funzionamento si basa sul meccanismo *"if this…then"*. Il concetto sarà comunque illustrato più diffusamente nel paragrafo 2.3.

[366] Finck, "Blockchain technology", (n. 364), 6-7. La funzione di *hash* è una tecnica di criptazione che consente di trasformare dei dati in una stringa di caratteri a grandezza fissa, a prescindere dalla mole dei dati da cui si parte. Il risultato viene definito come codice *hash*.

[367] Ibid, 20.

[368] Quando un nuovo partecipante entra a far parte della catena, aderisce al protocollo, che non costituisce altro che l'insieme delle regole scelte per la gestione delle transazioni eseguite *on-chain*. Questo meccanismo comporta che, ad esempio, prima che un nuovo nodo venga creato, ciascun utente sarà tenuto a dare il proprio consenso, in maniera tale da assicurare che la versione dei dati registrata su ciascun blocco sia corretta e identica. La trasparenza è incrementata anche dal fatto che ciascuna transazione è accompagnata da *un time-stamp*, cioè da un'indicazione sul momento esatto in cui è stata effettuata, e i dati saranno dunque ordinati secondo un ordine cronologico. Vi sono vari e diversi protocolli di consenso. Il più noto, utilizzato nelle *blockchain* come Bitcoin ed Ethereum, è il *proof-of-work*, che richiede a ciascun nodo di risolvere un problema matematico per validare le transazioni. Questo protocollo presuppone investimenti notevoli sia in termini di denaro che di energia, affinchè la catena sia effettivamente protetta contro eventuali attacchi. Il più noto è il cosiddetto attacco del 51%, reso possibile dal fatto che la maggior parte dei *miners* acquisti il controllo della catena e sia dunque in grado di gestire autonomamente il consenso. In alternativa a questo protocollo, viene spesso impiegato il *proof-of-stake*. Come suggerisce il nome stesso, i partecipanti dovranno "scommettere" sul sistema per partecipare alla formazione del consenso.

Con il termine *blockchain* si fa riferimento ad una famiglia di tecnologie e non ad una tecnologia singola, e le varie tipologie sono distinte l'una dall'altra da caratteristiche diverse[369]. Si distinguono infatti *blockchain* pubbliche o private, di tipo *permissioned* o *permissionless*. Nel caso di una catena pubblica e *permissionless*, chiunque ha la possibilità di possedere un nodo semplicemente scaricando il relativo software, senza ottenere alcun tipo di autorizzazione. Al contrario, una *blockchain* privata e *permissioned* si caratterizza per lo sfruttamento di sistemi come intranet o *virtual private network* (da qui in poi "VPN") e, pertanto, chi voglia acquistare un nodo dovrà preventivamente essere autorizzato da parte di un amministratore.

Come si vedrà meglio più avanti, la prima categoria garantisce di certo una maggiore trasparenza, ma pone maggiori problemi in termini di privacy, poiché chiunque ha la possibilità di scaricare e leggere interamente le transazioni registrate. La seconda categoria garantisce, invece, una maggiore tutela in tal senso e consente anche maggiore velocità nelle transazioni, poiché il numero di partecipanti coinvolti è inferiore ed è più facile raggiungere il consenso.

Queste combinazioni sono quelle attualmente prevalenti, ma nulla esclude che la catena possa assumere delle forme ibride. Un'altra categoria che sta iniziando a diffondersi è ad esempio quella delle catene consortili, condivise fra più soggetti che in tal modo abbattono i costi legati al mantenimento dell'infrastruttura e all'esecuzione delle transazioni, sebbene l'accesso alla catena sia comunque subordinato ad una forma di autorizzazione[370].

La catena può svolgere diverse funzioni partendo, alla pari degli altri registri distribuiti, dalla conservazione e gestione dei dati, sino all'impiego come infrastruttura per specifiche applicazioni, che generalmente replicano il carattere decentralizzato della *blockchain*[371]. Le diverse catene possono essere fra loro connesse ed interoperabili, creando delle strutture estese anche orizzontalmente[372].

La decentralizzazione e disintermediazione, che rappresentano due dei tratti maggiormente caratteristici di questa tecnologia, sono fra gli elementi destinati ad avere l'impatto più rilevante sull'economia, in quanto mettono in crisi i sistemi tradizionali che regolano le transazioni, basati sull'esistenza di un ente centrale, che gode della fiducia delle parti, ed è per questo investito del compito di validarle e assicurarne

[369] Ibid, 14-16.
[370] Visconti Moro (n. 333), 307.
[371] Finck, "Blockchain technology", (n. 362), 22.
[372] Questo genere di applicazioni è stato apprezzato soprattutto nel contesto della sharing economy, in cui l'idea di un'applicazione decentralizzata che sostituisca la piattaforma è assolutamente rivoluzionaria. Le decisioni normalmente rimesse all'uomo sarebbero infatti assunte dalla tecnologia stessa, secondo il protocollo di consenso scelto in origine, sostituendo alle regole giuridiche soluzioni di tipo tecnico. Pensare allo sviluppo di applicazioni che non rispettino la disciplina legale vigente, sarebbe però quantomeno pericoloso e ne renderebbe particolarmente complessa l'integrazione all'interno di imprese o altre realtà simili. La prospettiva più auspicabile per il futuro sarebbe dunque quella di costruire sistemi che facciano propri i principi attualmente sanciti a livello regolamentare, favorendo lo sviluppo di soluzioni tecniche compatibili e rispettose dell'attuale disciplina.

la correttezza[373]. Il concetto di fiducia in *blockchain* cambia invece radicalmente. Questa non è più riposta in un soggetto specifico, ma nella tecnologia stessa[374].

Ci si è largamente interrogati sulla possibilità di applicare la normativa vigente alla tecnologia *blockchain*, avendo ben presenti i problemi legati al fatto che le regole attualmente diffuse sono concepite nell'ottica di sistemi centralizzati, strutturalmente diversi rispetto a questa[375]. Ci si è mossi dunque nel senso di esplorarne la compatibilità, valutando al contempo la necessità di intervenire sul piano legislativo.

A livello europeo non è stato ancora elaborato un quadro normativo preciso volto a regolamentare questa nuova tecnologia, anche se qualcosa inizia a muoversi a livello nazionale in alcuni Stati Membri. In Italia, ad esempio, il D.L 14 dicembre 2018 n. 135, noto come Decreto Semplificazioni, ha introdotto all'art. 8*ter* la prima definizione normativa di *blockchain*[376] e *smart contract*. Sebbene l'introduzione di tale disposizione manifesti la volontà del legislatore di guidare lo sviluppo di queste nuove tecnologie entro i confini certi della legge e sia da questo punto di vista senz'altro apprezzabile, non sono pochi gli aspetti che hanno destato perplessità e sollevato critiche da parte della dottrina.

In primo luogo, la definizione utilizza la locuzione "architetturalmente decentralizzato su basi crittografiche", eppure né a livello giuridico che informatico è possibile rivenire ad una definizione certa di basi crittografica, con la conseguenza che l'interpretazione di tale dicitura risulta eccessivamente ambigua[377]. Inoltre la decentralizzazione va riferita all'accesso al registro e non al registro in sé. Contrariamente, una *blockchain* come Bitcoin sarebbe paradossalmente esclusa dalla definizione in esame. Non viene poi fatta menzione del protocollo del consenso che è invece centrale per il

[373] Finck, "Blockchain technology" (n. 362), 18-19.

[374] Se questo è assolutamente vero in linea teorica, bisogna però constatare che a livello pratico la governance della catena può essere anche centralizzata, e anzi lo è nella maggior parte dei casi. Per comprendere meglio questo aspetto, occorre tenere presente la distinzione fra il livello software e livello hardware, poichè che la centralizzazione può essere realizzata su uno o l'altro livello, o anche su entrambi. Quando si ha centralizzazione solo a livello software, nonostante la struttura sia effettivamente composta da una catena di blocchi decentralizzati, la governance è affidata soltanto a pochi soggetti. Questo è quello che avviene soprattutto nel caso delle blockchain permissioned, la cui gestione è rimessa ad un singolo o ad un piccolo consorzio di nodi. Anche nel caso delle blockchain permissionless (e il riferimento è sicuramente alle più note come Bitcoin e Ethereum), di solito considerate l'esempio tipico di decentralizzazione, si può dire che a livello software la gestione è in mano soltanto a pochi soggetti. Questo è dovuto al fatto che la decentralizzazione, pur portando con sé numerosi vantaggi, rende al contempo più complessa e meno efficiente la gestione delle transazioni, specialmente alla luce del fatto che queste possono facilmente estendersi su scala globale. In questo modo emergono infatti problemi nell'individuare la disciplina legale applicabile e la giurisdizione competente.

[375] Michèle Finck, "Blockchain as a regulatable technology" in *Blockchain Regulation and Governance in Europe*, (2019, Cambridge: Cambridge University Press,), 35, accessibile da https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04.

[376] D.L. n. 135/2018, "Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili". La definizione scelta dal legislatore italiano richiama quelle elaborate anche in altri Paesi. Fra le più note vi sono quella dello Stato dell'Arizona (USA) e quella elaborata dalla Digital Innovation Authority di Malta nel 2018.

[377] Francesco Contaldo, Flavio Campara, Donato A. Limone, e altri, "Blockchain, Criptovalute, Smart Contract, Industria 4.0: Registri Digitali, Accordi Giuridici e Nuove Tecnologie", 2019, (Pisa, Pacini giuridica), 145 ss.

funzionamento della catena. Un altro elemento dubbio è il riferimento alla non alterabilità e modificabilità dei dati, caratteristiche tipiche della *blockchain* ma non in generale di tutti i registri distribuiti, che possono possederle, ma non necessariamente con lo stesso grado di certezza garantito dalla *blockchain*. La definizione così elaborata rischia di risultare addirittura contraddittoria, laddove da un lato fa riferimento all'aggiornamento – e dunque alla modifica – dei dati e dall'altro parla di immutabilità degli stessi. Infine, nei termini in cui è posta la definizione sembra riferirsi esclusivamente alle *blockchain* di tipo *permissionless*.

2.2.2 Blockchain e GDPR: i rischi per i dati personali.

Si è detto che la *blockchain* è un registro distribuito sul quale vengono registrati dati, fra i quali possono naturalmente esservi anche dati personali. Sono però stati sollevati molti dubbi sulla compatibilità della *blockchain* rispetto alla disciplina dettata dal GDPR, anche in ragione del fatto che questa sia stata elaborata tenendo conto delle caratteristiche dei sistemi centralizzati[378]. Si è dunque cercato di analizzare se e in che misura la loro conciliazione sia possibile, come dimostra lo studio pubblicato dal Gruppo di Ricerca del Parlamento Europeo nel 2019[379]. Si è intuito, infatti, che l'avvento di questa nuova tecnologia potrebbe realmente rivoluzionare il modo di conservare e trasferire i dati, e nell'ottica di un'economia in cui questi ultimi hanno e avranno sempre più assoluta centralità, ignorarne l'importanza sarebbe non solo inutile, ma addirittura pericoloso. La tutela del diritto fondamentale alla protezione dei dati, insieme alla crescita dell'economia ed allo sviluppo di una tecnologia sostenibile, non può prescindere dallo studio di queste nuove realtà.

Nel condurre quest'analisi bisogna anzitutto tenere conto delle differenze esistenti fra le varie tipologie di *blockchain*, a partire dalla distinzione fra quelle di tipo *permissioned* e *permissionless*. In linea generale, si può dire che una valutazione corretta richiede un'analisi svolta caso per caso.

A. Ambito di applicazione del GDPR

Partendo dall'ambito di applicazione territoriale, s'intuisce facilmente che nel caso di *blockchain* pubbliche e *permissionless* sarà senz'altro più complesso per le autorità competenti sapere con certezza dove si trovi il titolare o il responsabile del trattamento e/o dove questo abbia luogo[380]. Da un lato, vi è incertezza (come si avrà modo di vedere meglio più avanti) su chi siano i soggetti qualificabili come

[378] Michèle Finck, "Blockchain and the General Data Protection Regulation" in Blockchain Regulation and Governance in Europe, (2019, Cambridge: Cambridge University Press,), 89, accessibile da https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04.
[379] EPRS, (n. 141).
[380] Ibid, 9-10.

titolari del trattamento e tale incertezza si riflette naturalmente anche sulla corretta individuazione dell'ambito di applicazione. Dall'altro, il modo in cui avvengono le transazioni sulla catena e il fatto che possano aggiungersi continuamente nuovi partecipanti di diversa collocazione geografica, complica ulteriormente la situazione. Al contrario, nel caso di *blockchain permissioned*, è più semplice individuare dove si trovi lo stabilimento principale al quale fare riferimento.

Per quanto riguarda invece l'ambito di applicazione materiale, va anzitutto chiarito che l'interpretazione estensiva del termine "trattamento dei dati" consente di ricomprendervi qualunque tipo di azione compiuta su di essi. Nel caso della *blockchain*, si parlerà dunque di trattamento dei dati sin dalla fase iniziale di caricamento di questi ultimi sulla catena, ricomprendendovi poi la conservazione e il trasferimento fra i vari nodi.

Anche nel contesto della tecnologia *blockchain* possono inoltre essere richiamate le questioni relative alla distinzione fra dati personali e no, insieme alle riflessioni già svolte sulla crescente possibilità di re-identificazione legata allo sviluppo delle nuove tecnologie. Parlando di *blockchain* il discorso s'incentra soprattutto sulle tecniche di anonimizzazione e/o pseudonimizzazione dei dati. Ciascun utente che opera sulla *blockchain* ha a propria disposizione una chiave pubblica, condivisa con tutti gli altri utenti, ed una chiave privata che può invece essere assimilata ad una password. Quest'ultima serve a decriptare i dati che sono stati criptati utilizzando la prima. Ciò che qui interessa stabilire è se le chiavi pubbliche possano o meno essere qualificate come "identificativi", ai sensi del *Considerando 30* del GDPR[381]. Si tratta di elementi che, se posti in relazione ad altre informazioni, consentono di identificare un soggetto specifico. La risposta è affermativa, almeno nell'ipotesi in cui i dati criptati facciano riferimento ad una persona fisica[382]. Dalla correlazione delle chiavi pubbliche con altri elementi, quali ad esempio il nome o l'indirizzo, è possibile identificare il soggetto interessato, motivo per cui tali dati saranno qualificabili come dati pseudonimi e non certo anonimi. In virtù del principio di responsabilità, i titolari del trattamento avranno l'onere di porre in essere tutte le misure tecniche ed organizzative che consentano di ridurre la possibilità di identificazione dei soggetti, ad esempio limitando la possibilità di incrociare i dati presenti sulla *blockchain* con quelli contenuti all'interno di altri *datasets*. Anche in questo caso, le *blockchain permissioned* e private si prestano più facilmente ad un'applicazione coerente con i principi dettati dal GDPR[383]. I dati diversi dalle chiavi pubbliche vengono definiti come dati transazionali[384]. Anche con riguardo a questi ultimi occorre chiedersi se possano essere qualificati o meno come dati

[381] GDPR, Considerando 30, "Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle".

[382] EPRS, (n. 141), 26.

[383] Ibid, 28.

[384] Ibid, 29-31 e Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 90.

personali. Alla luce dell'interpretazione estensiva che si suole dare di tale nozione, può tendenzialmente rispondersi in senso affermativo, anche se è opportuno fare delle precisazioni con riguardo al modo in cui i dati sono caricati sulla catena. Sia le chiavi pubbliche che i dati transazionali possono infatti essere caricati sotto forma di testo normale, in forma criptata o utilizzando un codice *hash*. Nel primo caso, quando tali dati fanno riferimento ad una persona fisica, sono sicuramente qualificabili come dati personali. Specialmente se si pensa al caso delle *blockchain permissionless* e pubbliche, i dati caricati in questo formato possono infatti essere facilmente letti da chiunque, elemento che mal si concilia con le esigenze di tutela dei dati poste dal GDPR. Negli altri casi occorre fare delle specificazioni.

Nel caso di dati criptati vi saranno dei soggetti in grado di decriptarli perché in possesso della chiave necessaria. Guardando ai dati dal loro punto di vista, questi rappresentano dunque dati personali, poiché consentono in ogni caso l'identificazione del soggetto a cui si riferiscono.

Più complesso è il discorso nel caso in cui i dati vengano caricati utilizzando una funzione di *hash*[385]. Nonostante in questo caso potrebbe giungersi più facilmente alla conclusione che i dati così trattati siano assolutamente anonimi, è pur vero che basterebbe immettere in un altro sistema che utilizza la stessa funzione i dati che si sa essere presenti su quella catena, per sapere a che stringa di caratteri corrispondono.

In conclusione, per determinare se i dati trattati possano essere considerati o meno come dati anonimi, è auspicabile che venga condotta un'analisi caso per caso, che tenga conto di tutte le circostanze concrete. Resta ferma comunque la considerazione che queste tecniche rientrano fra le misure da adottare auspicabilmente per accrescere il livello di sicurezza dei dati. In ogni caso è ben possibile che non tutti i dati siano conservati all'interno della catena, ma la *blockchain* può coesistere con altri *databases*, in cui questi sono raccolti. Per garantire una piena tutela dei dati personali si è spesso argomentato che questi dovrebbero essere conservati *off-chain* e legati alla catena soltanto mediante un puntatore *hash*. In tal caso la piena tutela dei dati conservati all'esterno della catena dovrà essere affidata ad un soggetto terzo che gode della piena fiducia delle parti[386]. Graverà invece sugli sviluppatori l'onere di garantire che anche i metadati, laddove siano in grado di rivelare informazioni personali, siano adeguatamente trattati.

B. Le basi giuridiche del trattamento

[385] Accanto alla funziona base di *hash*, ne esistono altre più complesse e sofisticate, come il *salted hash* e il *peppered hash*, che garantiscono maggiore sicurezza in quanto aggiungono valori ulteriori ai dati iniziali prima di convertirli. Nonostante ciò, lo stesso Gruppo di Lavoro Art. 29 ha evidenziato che esistono margini per consentire la re-identificazione dei soggetti e i dati in questione non possono pertanto essere considerati anonimi in modo irreversibile.

[386] Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 95.

a) Il consenso

L'applicazione dell'art. 6 del Regolamento, che individua le basi giuridiche che possono legittimare il trattamento dei dati, pone non pochi problemi anche con riguardo alla tecnologia *blockchain*. A partire dal consenso, la compatibilità fra quest'ultima e la disciplina del GDPR fa emergere molti dubbi[387]. In primo luogo non può sostenersi la tesi secondo cui sia sufficiente, ad esempio, avere acconsentito ad una transazione in Bitcoin perché possa dirsi che un soggetto abbia implicitamente prestato il proprio consenso al trattamento dei dati, posto che il GDPR è più che chiaro nello stabilire che questo debba essere prestato in forma esplicita. Un diverso problema è posto poi dal fatto che i dati, una volta entrati a far parte della catena, continueranno ad essere trattati finché il registro continua ad esistere. Non può dunque assicurarsi il rispetto del diritto di ritirare il consenso previamente prestato. Di conseguenza, il consenso può costituire una valida base giuridica per il trattamento dei dati mediante *blockchain* esclusivamente nell'ipotesi in cui vengano introdotti meccanismi che garantiscano all'interessato il diritto effettivo a ritirare il proprio consenso.

b) L'esecuzione di un contratto

Il trattamento dei dati personali mediante *blockchain* potrebbe essere legittimato ai sensi dell'art. 6 comma 1 lett. b) qualora esista fra le parti una relazione commerciale e/o contrattuale che lo giustifichi. Ad esempio, qualora una banca utilizzasse la *blockchain* per eseguire le proprie obbligazioni nei confronti dei clienti, la base giuridica qui in esame potrebbe certamente trovare applicazione[388].

c) Adempimento di un obbligo legale

L'art. 6 comma 1 lett. c) del GDPR dispone che il trattamento dei dati sia legittimo se necessario all'adempimento di un obbligo legale a cui è soggetto il titolare del trattamento. Nel caso della blockchain, questa disposizione potrebbe utilmente trovare attuazione, ad esempio, nel caso in cui i dati siano trattati in ottemperanza alle procedure richieste per il Know Your Customer (da qui in poi "KYC") o in ossequio alla normativa di antiriciclaggio[389].

d) Legittimo interesse

[387] EPRS, (n. 141), 61.
[388] Ibid, 62.
[389] Ibid, 62.

Il ricorso al legittimo interesse come base giuridica che legittimi il trattamento dei dati personali presuppone, ai sensi del considerando 47 del GDPR, che vi sia una relazione appropriata e rilevante fra il titolare del trattamento e il soggetto interessato, e che quest'ultimo possa ragionevolmente aspettarsi che il trattamento dei dati abbia luogo. Tuttavia, la disciplina non dà ulteriori indicazioni in merito al criterio di ragionevolezza a cui si fa riferimento e ciò rende complesso nella prassi individuare i casi concreti in cui questa base giuridica possa essere richiamata. Ad esempio, autorizzando l'esecuzione di una transazione sulla catena potrebbe ritenersi ragionevole che ciò comporti il trattamento di dati personali quali le chiavi pubbliche[390]. In realtà, si obietta che gli utenti non sono sempre consapevoli del fatto che le chiavi pubbliche siano qualificabili come dati personali. Maggiore chiarezza della disciplina e il rafforzamento degli obblighi informativi potrebbero allora contribuire ad un utilizzo corretto del legittimo interesse come base giuridica.

C. I principi e i diritti dell'interessato

a) Il principio di trasparenza e il diritto di informazione

Fra i principi dettati dall'art. 5 del Regolamento, particolare importanza va riconosciuta al principio di trasparenza, direttamente collegato ai diritti di informazione di cui gode l'interessato ai sensi degli articoli 13 e 14[391]. Ciò che qui occorre notare è che in ossequio al principio in esame non sussiste alcun obbligo specifico di mettere al corrente l'interessato sul fatto che il trattamento implichi l'utilizzo della tecnologia *blockchain*, purchè questo sia pienamente consapevole dei rischi in cui incorre. Anche in questo caso sarà opportuno condurre un'analisi caso per caso finalizzata ad accertare se tutte le misure necessarie a ridurre il rischio siano state o meno poste in essere.

b) Il principio di limitazione delle finalità

Più problematico è il rispetto del principio di limitazione delle finalità. Il GDPR prevede, infatti, che i dati possano essere legittimamente trattati solo per il fine originariamente comunicato all'interessato o, al più, per ogni altro fine ragionevolmente compatibile con esso[392]. Una volta presenti sulla catena, i dati continueranno ad essere trattati e coinvolti in transazioni ulteriori. Ciò che occorre stabilire è se quest'ulteriore trattamento sia compatibile con il fine originario o meno. Dovrà procedersi con un'analisi di tipo sostanziale piuttosto che meramente teorica, valutando la relazione esistente fra il fine originario e quello ulteriore, il contesto in cui i dati sono stati raccolti e ciò che l'interessato poteva ragionevolmente

[390] Ibid, 64.
[391] Ibid, 64.
[392] Ibid, 65.

aspettarsi, la natura dei dati trattati e le conseguenze del trattamento ulteriore e, infine, le misure poste in essere dal titolare per limitare l'impatto negativo sul soggetto interessato.

Quest'ultimo elemento impone di porre particolare attenzione alle conseguenze del trattamento dei dati nel caso di *blockchain* pubbliche, che di fatto comporta la loro condivisione dei dati con un pubblico vastissimo. Si tratta di un fattore di grande rilevanza, con un impatto notevole per l'interessato. Un problema simile sorge anche in relazione al principio di limitazione nella conservazione dei dati, in virtù del quale i dati possono essere conservati fintanto che siano necessari al perseguimento del fine per cui sono stati raccolti. Le incertezze sulle finalità del trattamento si ripercuotono dunque anche sull'applicazione del principio in esame.

c) Il principio di minimizzazione dei dati

Le caratteristiche intrinseche della *blockchain* si rivelano inoltre problematiche anche in relazione al principio di minimizzazione dei dati[393]. Da un lato, l'eliminazione dei dati caricati sui registri distribuiti è possibile solo in casi ed a condizioni eccezionali, con la conseguenza che questi tendono ad aumentare continuamente. Dall'altro, ciascun nodo della catena possiede una copia dell'intero registro, dando vita ad una infinita moltiplicazione dei dati, in assoluta contraddizione con quanto stabilito dal GDPR. Occorre valutare in che misura il trattamento dei dati *off-chain* possa contribuire a garantire il rispetto di tale principio, poiché ad esempio questo faciliterebbe la cancellazione dei dati.

d) Il diritto di accesso

Quanto al diritto di accesso ai dati sancito dall'art. 15 GDPR, potrebbe verificarsi che il titolare a cui l'interessato si rivolge – ad esempio uno dei nodi – non sappia effettivamente se i dati personali di quest'ultimo siano soggetti a trattamento o meno[394]. Se questi ultimi sono stati pseudonimizzati mediante criptografia, è inoltre difficile immaginare in che modo possa trovare concreta applicazione il terzo comma dell'articolo, che attribuisce all'interessato il diritto di ottenere una copia dei dati soggetti a trattamento. In ogni caso il titolare non può avere piena certezza dei soggetti a cui i dati saranno trasferiti, nonostante questo sia una delle informazioni a cui l'interessato ha diritto di accedere. In linea generale, soltanto l'implementazione di soluzioni tecniche adeguate – ed anche stavolta quella più accreditata rimane la conservazione dei dati *off-chain* – consentirebbe il pieno rispetto della disciplina.

[393] Ibid, 68; Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 104.
[394] Ibid, 72; Ibid., 106.

e) Il diritto alla rettificazione dei dati

Per quanto concerne il diritto alla rettificazione dei dati, riconosciuto ai sensi dell'art. 16 GDPR, occorre ancora una volta distinguere a seconda che si operi su una *blockchain permissioned* o *permissionless*[395]. L'esercizio di tale diritto sarà senz'altro più agevole nel primo caso, nel quale la sua effettività dipenderà essenzialmente dalle opzioni di *governance* scelte dai partecipanti. Nel caso di catene *permissionless*, invece, assicurare una piena tutela dell'interessato, sebbene possibile in linea teorica, è molto complesso nella prassi. Sarebbe infatti necessario che tutti i nodi della catena concordino nel creare un *fork*, cioè una deviazione rispetto alla catena iniziale, apportando ai dati le modifiche richieste dall'interessato. A ciò si aggiunga che l'interessato dovrebbe rivolgere la propria richiesta a ciascuno dei nodi, il che risulterebbe per lui estremamente oneroso. L'art. 16 attribuisce inoltre all'interessato il diritto ad ottenere l'integrazione dei dati incompleti. Interpretando tale diritto in senso finalistico, la valutazione dovrà tenere conto delle finalità per cui i dati erano stati originariamente raccolti e trattati. È dubbio se, alla luce di queste considerazioni, sarebbe dunque sufficiente che l'interessato ottenga l'inserimento nella catena dei nuovi dati corretti, fermo restando che i dati precedentemente inseriti non saranno comunque cancellati. Chi sostiene questa tesi sottolinea che il diritto alla rettificazione dei dati rimane comunque distinto da quello alla cancellazione e non sempre può ravvisarsi un reale interesse del soggetto in tal senso. La soluzione a queste questioni passerà ancora una volta sia dallo sviluppo di nuove soluzioni tecniche, ad esempio la conservazione dei dati *off-chain*, che dall'adozione di meccanismi di *governance* adeguati. Infine, un ulteriore elemento di difficoltà è posto dall'art. 19 GDPR, a norma del quale il titolare del trattamento ha l'obbligo di comunicare l'avvenuta rettificazione o cancellazione dei dati a tutti i soggetti terzi con cui questi sono stati condivisi. Nel caso di dati condivisi mediante *blockchain* non solo quest'obbligo potrebbe essere eccessivo, ma potrebbe anche rivelarsi impossibile da adempiervi.

f) Il diritto alla cancellazione dei dati

Il diritto alla cancellazione dei dati, noto anche come diritto all'oblio, è quello, almeno in apparenza, maggiormente problematico parlando della tecnologia *blockchain*. La cancellazione dei dati dal registro è infatti particolarmente complessa proprio in ragione degli elementi che caratterizzano quest'ultima[396]. Inoltre, anche se da un punto di vista tecnico la cancellazione dei dati può realizzarsi, vi sono difficoltà ulteriori legate al tipo di *governance* scelto dai partecipanti della catena. Alla pari di quanto si è detto in relazione al diritto di rettificazione, soltanto con il consenso di tutti i nodi la cancellazione di fatto aver luogo. Le soluzioni prospettate, su cui si sono confrontate diverse autorità nazionali competenti, a partire

[395] Ibid, 73; Ibid., 105.
[396] EPRS, (n. 141), 74-78; Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 107-108.

dall'ICO e dal Commission nationale de l'informatique et des libertés (da qui in poi "CNIL"), sono diverse e più o meno rilevanti a seconda del significato che si sceglie di attribuire alla nozione di cancellazione. Un'interpretazione strettamente letterale vanificherebbe gli effetti della stragrande maggioranza delle soluzioni prospettate, mentre attribuendo alla norma un significato più ampio – comunque non escluso dal GDPR – si avrebbe un maggiore margine di manovra. Questo secondo approccio si concilia inoltre con le istanze del GDPR circa la necessità di tenere conto della tecnologia esistente ed elaborare soluzioni ad essa compatibili. La soluzione più semplice sarebbe quella di rendere i dati anonimi ma, come visto, questo non è sempre semplice da realizzare in concreto.

Un'altra ipotesi sarebbe quella di distruggere le chiavi private, così che i dati sulla catena non potrebbero essere più decriptati. Qualunque sia la soluzione tecnica che si sceglie di adottare, questa dovrà comunque essere accompagnata da un modello di *governance* sostenibile e non sempre facile da configurare, motivo per cui è auspicabile un'analisi condotta caso per caso, alla luce della quale potrà dirsi con certezza se il diritto di cui all'art. 17 GDPR è garantito o meno. Tale analisi dovrà tenere conto dell'interpretazione che la CGUE[397] ha dato della norma, chiarendo che quello in esame non si configura come un diritto assoluto, ma va bilanciato con l'interesse dell'impresa a mantenere certi dati[398]. Si dovrà poi constatare se la registrazione dei dati sulla catena sia proporzionale e funzionale all'interesse perseguito nel momento in cui l'interessato richiede l'applicazione della norma.

e) Il diritto alla portabilità dei dati

Al diritto alla portabilità dei dati viene riconosciuta centrale importanza anche con riguardo alla tecnologia *blockchain*[399]. I problemi maggiori sono legati al fatto che i cosiddetti effetti *network* si manifestano anche in questo caso, scoraggiando l'esercizio del diritto. È assolutamente indispensabile incoraggiare lo sviluppo di sistemi fra loro interoperabili, affinchè il diritto alla portabilità possa concretamente essere esercitato.

C. Il titolare e il responsabile del trattamento

a) Il titolare del trattamento

[397] CGUE, C-131/12, Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González [2014].
[398] Moerel Lokke, "Blockchain and Data Protection" in Di Matteo, Larry A., Michel Cannarsa, and Cristina Poncibò The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, (2020, Cambridge: Cambridge University Press,), 228, accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.
[399] EPRS, (n. 141), 81.

Applicare la disciplina del GDPR implica individuare il soggetto che può essere qualificato come titolare del trattamento, cioè colui che ne determina le finalità e i mezzi. Anche se questi due elementi sono previsti in senso egalitario dal GDPR, nell'interpretazione corrente prevale l'idea che il criterio della finalità abbia una rilevanza maggiore di quello dei mezzi. Può richiamarsi anche in questo contesto, come si è fatto per i sistemi IoT, la necessità di adottare un approccio funzionale, verificando caso per caso chi sia effettivamente nella posizione di assumere tali decisioni. Nel caso della *blockchain*, può essere considerato come titolare del trattamento il soggetto che decide di ricorrere a tale tecnologia per il trattamento dei dati. Scegliere di utilizzare la *blockchain* equivale infatti a decidere come i dati saranno trattati[400]. In molti casi, soprattutto alla luce dell'interpretazione estensiva del concetto di controllo elaborata dalla giurisprudenza, finalizzata ad assicurare la più ampia tutela possibile agli interessati, potranno configurarsi forme di controllo congiunto. Non è tuttavia ben chiaro quale sia il grado di coinvolgimento richiesto perché questo possa effettivamente ritenersi esistente, né quale criterio prevalga nel riparto di responsabilità. Facendo un'analogia con quanto stabilito per il *cloud computing*, dovrebbero figurare come titolari del trattamento tutti i soggetti in grado di esercitare un controllo sul *software*, sull'*hardware* o sui centri di dati utilizzati per svolgere operazioni sulla catena. Nel caso delle *blockchain* che fungono quindi da infrastrutture per il funzionamento specifiche *app*, il titolare del trattamento è generalmente identificato con il soggetto che determina le modalità e fini del trattamento ad esse ricollegato. Una distinzione va fatta anche in questo caso fra *blockchain permissioned* e *permissionless*[401]. Nelle prime, è ragionevole attribuire il ruolo di titolare del trattamento all'entità o al consorzio di soggetti che controllano la catena. Più complesso è il discorso nel caso delle *blockchain permissionless*, rispetto alle quali vi è chi addirittura sostiene che, non potendosi identificare con certezza il proprietario della catena, non vi sarebbe alcun titolare o. seguendo una tesi diametralmente opposta, che tutti i nodi potrebbero parimenti essere qualificati come tali. Con un approccio più cauto, bisogna anzitutto scegliere la prospettiva più adeguata per individuare l'effettivo titolare. Ad un macro-livello il fine del trattamento è quello di fornire il servizio, mentre i mezzi utilizzati coincideranno con i *software* a disposizione dei nodi. Ad un micro-livello, invece, il fine consiste nel porre in essere una singola transazione e il mezzo coincide con la scelta della piattaforma *blockchain*. Questo secondo punto di vista sembra essere quello più adatto per identificare con certezza il titolare del trattamento. È in ogni caso opportuno svolgere un'analisi più dettagliata e concreta, guardando con maggiore attenzione ai soggetti coinvolti e al livello di controllo da essi esercitato.

Si guardi in primo luogo agli sviluppatori dei *software*. Sebbene questi ne definiscano il design, non hanno una reale influenza sulla scelta di porre in essere o meno gli aggiornamenti, né assumono decisioni

[400] Ibid., 39-48.

[401] Si veda diffusamente Nicola Fabiano, "Blockchain and Data Protection: The Value of Personal Data", (2018), vol. 16 no. 6 Journal of Systemics, Cybernetics and Informatics, accessibile da http://www.iiisci.org/Journal/CV$/sci/pdfs/ZA165NO18.pdf; Lokke, (n. 398), 215-216.

sul trattamento specifico di alcuni dati, limitandosi a mettere a disposizione di altri la tecnologia. Tendenzialmente è dunque da escludersi che possa attribuirsi loro il ruolo di titolari del trattamento. I *miners* sono invece coinvolti nella creazione di nuovi nodi secondo il protocollo scelto dalla catena e conservano una copia dello storico delle transazioni. Scegliendo quale versione del protocollo attivare, questi hanno senz'altro un controllo sui mezzi del trattamento, ma restano comunque estranei alla determinazione dei fini. Nell'individuazione concreta del titolare ad assumere rilevanza maggiore è però proprio questo secondo elemento. Il fatto che l'attività dei *miners* non dia loro alcun controllo sullo scopo per cui i dati vengono trattati, porta a concludere che la loro qualificazione come titolari sia quantomeno inopportuna, se non addirittura da escludersi. Il discorso cambia parlando invece dei nodi, cioè dei computer che partecipano alla *blockchain* conservando una copia della catena e che sono attivamente coinvolti nel processo di validazione dei blocchi. Potrebbe configurarsi in questo caso una forma di controllo congiunto, poiché ciascun nodo influenza allo stesso modo lo sviluppo della catena. Secondo la tesi opposta[402], in realtà ciascun nodo decide per sé e non è in grado di influenzare il trattamento dei dati posto in essere dagli altri. Mancherebbe la condivisione nella determinazione delle finalità e dei mezzi necessaria per poter configurare un controllo congiunto. In conclusione, ciascuno di essi dovrebbe autonomamente essere qualificato come titolare. L'incertezza sulla corretta interpretazione da dare alla nozione di controllo congiunto, non consente di assumere una posizione certa a riguardo. Né può ignorarsi che l'elevato numero di nodi coinvolti ne renderebbe molto difficile l'applicazione pratica. Un altro problema legato all'attribuzione del ruolo di titolare ai nodi risiede nel fatto che questi hanno accesso ai dati soltanto in forma criptata e non si comprende in che modo potrebbero concretamente adempiere agli obblighi imposti dalla disciplina del GDPR. Gli utenti, infine, sono le persone fisiche o giuridiche che sottoscrivono le singole transazioni sulla catena[403]. Quando una transazione è effettuata direttamente dall'utente, anche se si tratta di una persona fisica, questo dovrebbe essere qualificato come titolare del trattamento. Gli utenti potrebbero acquisire la qualifica di titolari con riferimento ai dati caricati sul registro e quella di responsabili in relazione alla copia del registro che conservano. Va in ogni caso fatta una distinzione a seconda che il trattamento abbia ad oggetti dati dell'utente stesso o dati relativi ad altri soggetti. Nel primo caso si potrebbe sostenere che operi la cosiddetta *"household exemption"*, escludendo dunque il trattamento dall'ambito di applicazione del GDPR. Dovendo garantire il massimo livello di tutela dei dati personali, è però preferibile escludere questa opzione, specialmente trattando di *blockchain permissionless* e pubbliche, in cui i dati sono facilmente accessibili da chiunque. Anche nel caso di *blockchain permissioned*, nella maggior parte dei casi il trattamento avviene comunque per il perseguimento di fini commerciali o professionali, e le regole dettate dal GDPR dovranno dunque applicazione. Il problema è legato al fatto che la disciplina europea non è sufficientemente chiara nel determinare se, ed eventualmente a quali condizioni, il soggetto

[402] Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 100.
[403] EPRS, (n. 141), 48-55.

interessato possa al contempo figurare come titolare del trattamento. Se da un lato questa opzione potrebbe essere concepita come un modo per attribuire maggior controllo sui propri dati personali all'interessato, secondo un indirizzo pienamente in linea con i princìpi dettati dal GDPR, dall'altro lato è alto il rischio che il trattamento avvenga in modo più irresponsabile, perché l'interessato non ha un livello di conoscenze adeguato e che gli consenta di comprenderne pienamente la complessità. Nel caso in cui il trattamento abbia invece ad oggetto dati riferiti ad un'altra persona, in linea con quanto stabilito sia per i *social network* che per il *cloud computing*, l'utente è qualificabile come titolare se agisce per il perseguimento di fini che lui stesso ha stabilito.

b) Il responsabile del trattamento

Anche l'individuazione del responsabile del trattamento necessita di una valutazione svolta caso per caso, al fine di determinare quale sia il grado di autonomia di ciascun soggetto e se possa ritenersi sussistente quel rapporto di subordinazione rispetto alle istruzioni impartite dal titolare che giustifica il degradamento del livello di responsabilità ad egli attribuibile[404]. Generalmente, la qualifica di responsabile viene attribuita alle piattaforme che mettono la *blockchain* a disposizione di altri (BaaS). Non dovrà invece darsi eccessivo rilievo alla necessità che il titolare e il responsabile del trattamento siano legati da un rapporto contrattuale, lasciando che l'allocazione delle responsabilità segua piuttosto ad un approccio funzionale. L'esistenza di un contratto potrebbe rivelarsi particolarmente problematica nel caso delle *blockchain permissionless*, in cui un vero potere contrattuale potrebbe essere configurato soltanto in capo agli sviluppatori che però, come si è visto, non sono qualificabili come titolari del trattamento.

D. Le decisioni automatizzate

La rilevanza dell'art. 22 e alla disciplina da esso dettata in relazione alle decisioni automatizzate è legata nel contesto *blockchain* soprattutto all'utilizzo degli *smart contract* che, almeno in alcuni casi, può ritenersi assumano delle vere e proprie decisioni aventi effetti legali, senza alcun intervento umano. La questione sarà dunque meglio approfondita nel prosieguo parlando di questa particolare categoria di contratti.

E. Privacy-by-design e privacy-by-default

[404] Ibid, 56.

Naturalmente, anche quando viene impiegata la tecnologia *blockchain* il titolare del trattamento sarà tenuto a rispettare i principi di *privacy-by-design* e *privacy-by-default* di cui all'art. 25 del GDPR[405]. Soltanto lo sviluppo di adeguate soluzioni tecniche, insieme all'elaborazione di un sistema di *governance* adeguato, può contribuire a garantire che l'utilizzo della *blockchain* sia pienamente compatibile con la disciplina sulla protezione dei dati personali. Non si dimentichi che il principio di *privacy-by-design* è la prova del favore che le istituzioni europee hanno mostrato verso la creazione di soluzioni innovative in grado di conciliare gli aspetti tecnici a quelli regolamentari, ed è proprio nel connubio fra tecnologia e legge che possono trovarsi le risposte alle esigenze del prossimo futuro[406]. L'incertezza deriva principalmente dal fatto che non esistono ancora delle soluzioni in grado di assicurare in maniera assoluto la tutela dei dati, anche se sono state proposte diverse misure che contribuiscono ad una effettiva riduzione dei rischi. Allo stato dell'arte, come si è più volte avuto modo di sottolineare, soltanto un'attenta analisi condotta caso per caso potrà consentire di determinare se il titolare abbia o meno posto in essere tutte le misure necessarie e auspicabili, tenuto conto delle difficoltà già esaminate nell'individuare con certezza a chi possa effettivamente essere attribuito tale ruolo. Fra gli obblighi a cui questo sarà soggetto rientrerà senz'altro, ai sensi dell'art. 35 GDPR, anche la predisposizione della DPIA, obbligatoria nell'ipotesi in cui il trattamento dei dati preveda l'impiego di una nuova tecnologia. Anche se si discute su quale sia il lasso di tempo rilevante entro cui può effettivamente dirsi sussistente un elemento di novità, al momento la tecnologia *blockchain* ricade sicuramente entro l'ambito di applicazione della norma e lo strumento in esame dovrà utilmente essere impiegato proprio per ridurre i rischi a cui il soggetto interessato è esposto.

Nonostante i profili critici sin qui evidenziati, va tenuto presente che la Commissione europea[407] ha individuato proprio nella *blockchain* una delle tecnologie che potranno maggiormente contribuire alla creazione alla sostenibilità del Digital Single Market, proponendola quale strumento innovativo di *governance* dei dati. La possibilità di creare delle reti di condivisione dei dati decentralizzate, nelle quali non è necessaria la presenza di un entità centrale che goda della fiducia dei partecipanti, l'intrinseca trasparenza di questi sistemi e la possibilità di dar luogo a transazioni automatiche grazie all'implementazione degli *smart contract*, sono tutti elementi che, a parere della Commissione, giocheranno un ruolo di primaria importanza nello sviluppo dei nuovi mercati digitali e dell'economia del futuro prossimo.

[405] Ibid, 85-87 e Finck, "Blockchain and the General Data Protection Regulation", (n. 378), 108-110.
[406] Lokke, (n. 398), 225.
[407] Commission, "Shaping Europe's digital future", accessibile da https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy.

La fiducia riposta in questa nuova tecnologia è testimoniata dal fatto nel 2018 ben 22 Paesi dell'Unione Europea, compresa l'Italia, hanno siglato un accordo per la creazione di un partenariato sulla *blockchain*, funzionale proprio alla costruzione del Digital Single Market.

2.3 Smart contracts: storia, funzioni e inquadramento giuridico dei nuovi contratti automatici.

Con il termine *smart contract* si fa riferimento ai cosiddetti contratti automatici. Il concetto è stato introdotto per la prima volta nel 1997 da Szabo, il quale descrisse questi nuovi contratti come "protocolli computerizzati che eseguono i termini di un contratto"[408].

Da un punto di vista tecnico gli *smart contract* non sono altro che codici informatici che contengono ed eseguono istruzioni specifiche. Date determinate premesse, seguirà un certo risultato, seguendo la logica del *"if this…then"*[409]. Non necessariamente assumono dunque il valore giuridico di un contratto, ma possono farlo se presentano specifiche caratteristiche. Non vi è conflitto fra la dimensione tecnica e quella giuridica, come confermato anche dal fatto che la dottrina ha paragonato la logica sottostante a tali contratti ad un sillogismo giuridico[410]. Se non presenta gli elementi necessari perché possa essere configurato come contratto, uno *smart contract* può comunque essere utilizzato per altri scopi, ad esempio dare semplicemente attuazione a specifiche istruzioni. Non bisogna poi commettere l'errore di reputare questi contratti "intelligenti" nel senso di riconoscere loro la capacità di agire autonomamente. Lo *smart contract* si limita infatti a dare esecuzione ad uno schema predeterminato.

Ad oggi gli *smart contract* sono generalmente associati alla tecnologia *blockchain* e all'impiego di sistemi AI. Nonostante l'indubbio vantaggio di utilizzare congiuntamente queste diverse tecnologie, è bene avere presente che gli *smart contract* possono esistere ed essere adottati anche in modo isolato[411]. Il loro stesso inventore, Szabo, aveva evidenziato che non vi è alcun obbligo di integrare gli *smart contract* con sistemi *machine learning*. Blockchain e *smart contract* si sposano però benissimo in quanto entrambi eliminano la necessità di coinvolgere parti terze nell'esecuzione delle transazioni, garantendone la massima sicurezza in virtù dell'immutabilità dei dati caricati su *blockchain*. Una volta

---

[408] N. Szabo, *Smart Contracts*, (1994).

[409] Letteralmente "Se questo…allora". Con questa formula si suole descrivere il meccanismo di funzionamento del contratto che, date specifiche premesse, produce un risultato predeterminato. L'esempio più semplice che si suole fare per spiegare il funzionamento di questi contratti è quello dei distributori automatici di cibo e bevande: ad una condizione precisa (l'inserimento delle monete e la digitazione del numero corrispondente al prodotto desiderato), la macchina esegue un determinato comando (erogazione del prodotto). (Valentina Gatteschi, Fabrizio Lamberti e Claudio Demartini, "Technology of smart contracts", in Di Matteo, Larry A., Michel Cannarsa e Cristina Poncibò *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, 2020, (Cambridge: Cambridge University Press), 42, accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.

[410] Contaldo, Campara, Limone, et al, (n. 377). 34.

[411] Riccardo De Caria, "Definitions of smart contracts – between law and code", in Di Matteo, Larry A, Michel Cannarsa, and Cristina Poncibò *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, 2020, (Cambridge: Cambridge University Press), 22-24, accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.

caricato sulla catena, il contratto non potrà infatti essere in alcun modo modificato o alterato e sarà eseguito automaticamente non appena si verificheranno le condizioni richieste. Ciò fa sì che non sia più necessario che esista un rapporto di fiducia fra le parti, perché questa sarà riposta piuttosto nella tecnologia stessa[412]. A grandi linee, potremmo descrivere il funzionamento degli *smart contract* riportandolo a due diversi schemi[413]. Si faccia l'esempio di un contratto di compravendita di un *asset* digitale. La parte X è obbligata a trasferire all'altra la proprietà dell'*asset*, mentre la controprestazione dovuta da Y consiste nel pagamento di una determinata somma di denaro. Accertato l'avvenuto trasferimento della proprietà, il contratto eseguirà immediatamente la controprestazione dovuta. Gli *smart contract* potrebbero però essere utilizzati anche con una diversa funzione, cioè quella di raccogliere informazioni da fonti esterne, elaborarle ed eseguire specifiche azioni. Queste fonti vengono chiamale "oracoli" e svolgono un ruolo di primaria importanza, in quanto costituiscono un ponte fra gli *smart contract* e la catena *blockchain* che ne regola il funzionamento e il mondo esterno. Questo rappresenta però anche un rischio per il sistema, dal momento che non vi è certezza sulla correttezza e l'integrità dei dati trasmessi. È importante dunque che si tratti di fonti affidabili e verificate, per evitare che, immettendo nella catena dati scorretti, il protocollo non venga eseguito correttamente. Per garantire maggiore sicurezza, normalmente i dati rilevati dagli oracoli non vengono immessi direttamente nella catena, ma sono prima soggetti ad un controllo finalizzato proprio ad accertarne la correttezza e la qualità. Le parti potrebbero anche preventivamente concordare a quali fonti riconoscere il potere di immissione dei dati, anche al fine di evitare che sorgano successivamente conflitti. Esistono varie tipologie di oracoli[414]. Si parla ad esempio oracoli *software/hardware* o *inbound/outbound*. La prima coppia di aggettivi distingue a seconda che la fonte da cui questi estraggono dati siano siti web o oggetti reali, facendo ricorso ad esempio all'utilizzo dei sensori. Come si vedrà meglio nel prossimo capitolo, i dispositivi che compongono i sistemi IoT potrebbero essere utilizzati proprio nella funzione di oracoli della catena.

Gli *smart contracts* potranno essere utilizzati per gestire le transazioni eseguite attraverso le applicazioni decentralizzate che sfruttano la *blockchain* o per dare esecuzioni alle regole di *governance* scelte da una *decentralized autonomous organization* (da qui in poi "DAO")[415]. Si tratta di particolari organizzazioni non verticistiche e che adottano un meccanismo decisionale automatizzato. La prima DAO è stata sviluppata nel 2014 dalla piattaforma Dash, ma il successo e la diffusione di queste organizzazioni si

[412] Max Raskin, "The Law and Legality of Smart Contracts", (2017), vol. 304 Georgetown Law Technology Review, 311, accessibile da https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2842258; Eliza Mik, "Smart Contracts: Terminology, Technical Limitations and Real World Complexity"', (2017), vol. 9/no. 2, Law, Innovation and Technology, 280, accessibile da https://www.tandfonline.com/doi/full/10.1080/17579961.2017.1378468.

[413] Contaldo, Campara, Limone, (n. 377), 37.

[414] Mik, (n. 412), 296 ss; Levi Stuart, Alex B Lipton, "An Introduction to smart contracts and their potential and inherent limitations", (2018, Harvard Law School Forum on Corporate Law), accessibile da https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/; Gatteschi, Lamberti e Demartini, (n. 409), 44.

[415] Contaldo, Campara, Limone, (n. 377), 66.

deve ad Ethereum, che nel 2016 ha lanciato "theDAO". Il suo funzionamento è legato da un lato proprio alla possibilità di sviluppare *smart contract* e dall'altro a quella di legittimare l'esecuzione di transazioni attraverso i diritti distribuiti mediante *token*. Le DAO si distinguono dalle più tradizionali *Decentralized Organization* (DO) perché il sistema di *governance* non è più impostato in maniera gerarchica e soggetto al rispetto di regole e codici di comportamento specifici, bensì decentralizzato e subordinato al rispetto delle regole aziendali registrate su *blockchain*[416]. È la catena a verificare la correttezza di ciascuna transazione, rendendo di fatto impossibile che queste si discostino dalle suddette regole. L'intervento umano è dunque limitato alla definizione delle regole iniziali, cioè dell'organizzazione, mentre la fase di controllo è demandata esclusivamente al software. L'organizzazione è in grado di agire con certo grado di autonomia, che rimane però costretto entro i limiti delle istruzioni impartite inizialmente. La gestione basata sull'impiego di algoritmi consente di raggiungere livelli di efficienza maggiori rispetto a quanto avviene nelle organizzazioni tradizionali[417]. Il sistema è infatti in grado di optare sempre per la decisione migliore da un punto di vista economico, senza essere condizionato da fattori esterni come accade spesso nel caso di decisioni assunte dall'uomo. In ogni caso l'efficienza economica è valutata dal sistema sulla base delle istruzioni preliminarmente impartite a quest'ultimo e non potrà dunque discostarsi dal fine che le parti hanno originariamente inteso perseguire. Da un lato la trasparenza del sistema è garantita dall'adozione di un *software open source* che consente ai partecipanti di partecipare alle operazioni svolte, ad esempio fornendo dati, *criptoasset* o acquistando servizi[418]. Dall'altro lato, l'autonomia della DAO si ravvisa nel fatto che questa continua ad operare finché vi è criptovaluta disponibile, indipendentemente dalla volontà dei suoi partecipanti. Per tale ragione la DAO potrebbe essere considerata come un centro d'imputazione a sé stante ed è estremamente importante capire se e in che misura questa possa essere ritenuta giuridicamente responsabile. Le norme del codice civile italiano non consentono di risolvere il problema, dal momento che in tal caso non potrebbe trovare applicazione né la disciplina di cui all'art. 38 c.c. in materia di associazioni non riconosciute, mancando di fatto la figura del legale rappresentante responsabile, né altre norme che presuppongono il riconoscimento della personalità giuridica. Piuttosto, la DAO potrebbe essere assimilata ad una comunione di beni, ed in questo caso la responsabilità ricadrebbe su ciascun partecipante in misura proporzionale ai *token* detenuti, senza però risolvere realmente la questione. Nel caso in cui venga violata una norma, si discute se a risponderne sia lo sviluppatore o l'utilizzatore del sistema o se la responsabilità vada imputata al sistema stesso. Naturalmente quest'incertezza incide negativamente sui proprietari dei *token*, che non possono considerarsi pienamente tutelati.

[416] Ibid., 67.
[417] Daniel Kraus, Thierry Obrist, Olivier Hari, e altri, "Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law", 2019, (Northampton, Ma, USA; Cheltenham, UK, Edward Elgar), 110.
[418] Contaldo, Campara, Limone, (n. 377), 66 ss.

2.3.1 Validità e inquadramento giuridico degli smart contract

Le caratteristiche proprie degli *smart contract* li differenziano sotto diversi aspetti dai contratti tradizionali. Alcuni ordinamenti, fra cui quello italiano, hanno tentato di dettare una disciplina volta a regolamentare questi nuovi strumenti ma, sebbene sia apprezzabile l'intenzione di chiarire il quadro giuridico, si tratta di interventi di carattere ancora embrionale e portata limitata. Inoltre, alla luce del fatto che gli *smart contracts* sono destinati ad essere utilizzati soprattutto in transazioni che presentano profili sovranazionali, sarebbe comunque auspicabile un intervento legislativo uniforme e di più ampio respiro, così da garantire una maggiore certezza del diritto e favorirne la diffusione[419]. L'esperienza di Internet ci ha insegnato che lo sviluppo delle nuove tecnologie non può prescindere da un loro parallelo inquadramento giuridico e che l'utilizzo della tecnologia al di fuori del sistema legale esistente si espone a possibili abusi e attacchi, perdendo la fiducia degli utenti, che finirebbero con il non utilizzarla.

Per quello che qui interessa, i problemi che sorgono dalle incertezze concernenti la validità e l'inquadramento giuridico degli *smart contract* vanno esaminati tenendo a mente un presupposto specifico. Come si vedrà meglio nel capitolo III, gli *smart contract* possono essere utilizzati per disciplinare il trattamento dei dati personali nei sistemi IoT. Chiarire quale sia la loro validità e il valore giuridico a questi attribuibile è dunque presupposto indefettibile perché venga garantito il rispetto del principio di liceità sancito dall'art. 5 del GDPR.

Il quadro normativo italiano

Il legislatore italiano ha introdotto la prima definizione normativa di *smart contract* all'art. 8*ter* nel D.L. 135/2018[420], congiuntamente a quella di *blockchain* e delle Distributed Ledger Technology (da qui in poi "DLT"), demandando all'Agenzia per l'Italia Digitale (da qui in poi "Agid") il compito di emanare entro 90 giorni le linee-guida che definissero i requisiti necessari perché gli *smart contract* possano soddisfare il requisito della forma scritta. Purtroppo l'Agid non ha però ancora provveduto in tal senso.

La definizione di *smart contract* elaborata dal legislatore italiano è imprecisa e fuorviante almeno sotto due diversi punti di vista[421]. In primo luogo, è inadeguato l'implicito riferimento all'art. 1321 c.c., reso evidente dall'utilizzo del termine "vincolare", nonché dall'aver fatto menzione di "due o più parti" e del requisito della forma scritta. Non vi è infatti alcun parallelismo fra la disciplina civilistica in materia

[419] Mik, (n. 412), 284.

[420] D.L. 135/2018, art. 8*ter*, comma 2. "Si definisce «*smart contract*» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contract* 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 del presente decreto".

[421] Contaldo, Campara, Limone, (n. 377), 148 ss.

contrattuale e la regolamentazione degli *smart contract* e, come si è già avuto modo di evidenziare, questi strumenti possono essere utilizzati anche per scopi ulteriori rispetto a quello di redigere contratti, ad esempio per l'automazione di determinati processi produttivi. La norma presenta un ulteriore elemento di imprecisione in quanto lega in maniera imprescindibile l'applicazione degli *smart contract* all'utilizzo di registri distribuiti o *blockchain*. Nonostante il legame fra le due tecnologie sia senz'altro di grande rilevanza, si tratta di un'inopportuna limitazione alla portata applicativa di questi strumenti, il cui impiego è invece assolutamente autonomo. Un altro elemento che ha destato non poche critiche da parte della dottrina è il riferimento all'esecuzione del contratto quale elemento che vincola le parti. L'espressione così come formulata dal legislatore sembrerebbe infatti contraddire il principio consensualistico che vige nel nostro ordinamento, in virtù del quale il vincolo fra le parti sorge già nel momento in cui queste assumono l'obbligazione e non in quello in cui il contratto viene eseguito. Il termine potrebbe anche ritenersi riferito all'esecuzione informatica del programma e il vincolo che ne deriva legato alla presunta immutabilità della *blockchain*. Seguendo questa interpretazione si finirebbe però col negare di fatto la libertà contrattuale delle parti, i cui rapporti sarebbero regolati direttamente e in modo esclusivo dalla tecnologia stessa. La disposizione tradisce inoltre il generale principio di neutralità tecnologica, facendo espresso riferimento ai registri DLT e alla *blockchain*. Se da un lato la scelta del legislatore mira a favorire ed incoraggiare gli investimenti in queste tecnologie, l'attuale formulazione della norma potrebbe rivelarsi eccessivamente limitante per futuri sviluppi.

L'esecuzione automatica del contratto: vantaggi e rischi

Il principale vantaggio legato agli *smart contract* è quello di eliminare i rischi legati ad un possibile inadempimento o alla malafede delle parti, riducendo al contempo i costi di transazione ed esecuzione del contratto. Questo perché non vi è bisogno dell'intervento di un soggetto terzo che operi in qualità di garante o con funzioni di controllo. La differenza con i contratti tradizionali si coglie nel fatto che mentre la loro forza è legata al valore giuridico e vincolante che viene loro attribuito dall'ordinamento e che legittima le parti a chiedere l'intervento dell'autorità giudiziaria o ricorrere agli rimedi disciplinati dal codice civile nel caso di inadempimento della controparte, nel caso degli *smart contract* l'intervento di un soggetto terzo è escluso, poiché è la tecnologia stessa a garantire che venga data esecuzione al contratto. La fiducia delle parti non è pertanto riposta nella tutela giuridica assicurata dall'ordinamento, quanto nell'architettura del contratto e nel suo meccanismo di funzionamento.

Il fatto che gli *smart contract* siano *self-enforcing* e *tamper-proof*, cioè che la loro esecuzione avvenga automaticamente e a prescindere dalle circostanze esterne al contratto, ha però anche dei lati negativi. Una volta che il contratto è stato stipulato, potrebbero infatti rendersi necessarie delle modifiche dei termini o la cessazione del contratto stesso. A differenza di quanto accade nei contratti tradizionali, le

parti non sono libere di decidere se e quando adempiere alle proprie obbligazioni contrattuali. Ad esempio, laddove sia entrata in vigore una nuova disposizione di legge prima che il contratto abbia avuto esecuzione, è necessario poter aggiornare e modificare i termini contrattuali in senso ad essa coerente[422]. Più in generale, bisogna presumere che al momento della stipulazione del contratto le parti non siano in grado di prevedere tutti i possibili scenari futuri e che quest'ultimo non contenga dunque le disposizioni necessarie per far fronte ai diversi possibili sviluppi. Per ovviare alle difficoltà in cui potrebbero incorrere per procedere alla modifica dei termini contrattuali, le parti dovrebbero preventivamente accordarsi per scegliere quali elementi saranno immutabili e quali invece no. Si tenga presente che l'esigenza di modificare il contratto può sorgere anche dal fatto che questo si riveli intrinsecamente scorretto o iniquo. Con un ragionamento parallelo a quello già fatto in merito agli algoritmi *machine learning*, non bisogna dimenticare che gli *smart contract* sono comunque creati dagli esseri umani e non sono certo immuni dall'inglobare eventuali errori e *bias*[423], intenzionali o determinati da un *bug* da cui è affetto il *software*. Problemi simili si pongono per quanto riguarda la possibilità di far cessare un contratto. In tutti questi casi le parti dovranno rivolgersi ad una corte o ad un arbitro per la risoluzione delle eventuali dispute, con la conseguenza che le decisioni relative alla vita del contratto verrebbero assunte al di fuori del contratto e/o della *blockchain* su cui questo viene eseguito.

Il linguaggio degli smart contract

Un altro importante limite degli *smart contract* è legato al linguaggio[424]. Alcune disposizioni, più semplici e lineari, con elementi di natura strettamente quantitativa, potranno infatti facilmente essere tradotte in codici informatici. Nella maggior parte dei casi, però, le clausole contrattuali sono ricche di espressioni dal significato ampio e volutamente ambigue, spesso scelte dalle parti per garantire un margine di flessibilità maggiore all'accordo. In questi casi fare ricorso agli *smart contract* può risultare non solo particolarmente complesso, ma addirittura tecnicamente impossibile e non auspicabile.

[422] Raskin, (n. 412), 327; Kraus, Obrist, Hari, et al, (n. 417), 117 ss.

[423] Ad esempio, la determinazione delle condizioni necessarie perché venga data esecuzione al contratto potrebbe derivare da un errore di valutazione di una delle parti o dal fatto che questa sia stata effettivamente tratta in inganno. Ammettendo che agli *smart contract* possa liberamente applicarsi la disciplina civilistica in materia di contratti, potrebbero in tal caso trovare applicazione le norme che regolano l'invalidità del contratto. Guardando nello specifico alla disciplina italiana, potrebbe essere richiamato l'art. 1428 c.c., che prevede la nullità del contratto nel caso di errore essenziale e riconoscibile. Le ipotesi di errore essenziale sono elencate dal successivo art. 1429 c.c, mentre l'art. 1431 c.c. definisce l'errore riconoscibile se la parte avrebbe potuto rilevarlo usando l'ordinaria diligenza. Le parti dovrebbero dunque sempre avere la possibilità di dimostrare di essere cadute in errore al momento della stipulazione, ottenendo la dichiarazione di nullità del contratto laddove sussistano le condizioni necessarie. L'automatica esecuzione del contratto renderebbe però praticamente impossibile l'operatività di questo sistema, lasciando alla parte caduta in errore la sola possibilità di ottenere un rimedio risarcitorio rivolgendosi ad una corte. Il discorso si complica ulteriormente pensando poi all'ipotesi in cui gli smart contract siano utilizzati non tanto per regolamentare il rapporto fra due persone fisiche, quanto nell'ambito di una relazione *machine-to-machine*. Si potrebbe infatti obiettare che in tal caso manchi il presupposto principale per l'applicazione della norma, ossia il vizio della volontà di una delle parti, poiché il contratto non dà attuazione alla volontà di una persona fisica, ma si limita a regolare l'attività dei dispositivi. Un errore nella formulazione dell'algoritmo potrebbe tuttavia rivelarsi egualmente pericoloso, ed è necessario poter comunque intervenire per porvi rimedio.

[424] Contaldo, Campara, Limone, (n. 377), 43-47; 56-57.

L'eccessiva rigidità del codice finirebbe infatti col limitare la libertà delle parti e il contratto non risponderebbe adeguatamente alle loro esigenze, a maggior ragione quando questo mira a disciplinare rapporti di lunga durata. Tali difficoltà si manifestano non soltanto nella fase di redazione del contratto, ma soprattutto in quella di interpretazione dello stesso. Nell'ordinamento italiano, a norma dell'art. 1362 c.c., l'interprete deve tenere conto, oltre che del dato letterale, anche della comune intenzione delle parti, manifestata anche grazie al comportamento tenuto da queste nella fase successiva alla stipulazione del contratto. È difficile immaginare come tale criterio interpretativo, che peraltro figura anche in ordinamenti diversi da quello italiano, possa in concreto trovare applicazione nel caso di un contratto ad esecuzione automatica e scritto secondo le regole del codice binario. L'utilizzo dei contratti automatizzati dovrebbe allora limitarsi alla regolamentazione delle sole ipotesi più semplici, in cui è possibile definire i termini del contratto con maggiore precisione. Nelle situazioni più complesse dovrebbero invece essere adottati contratti tradizionali per descrivere compiutamente la relazione fra le parti e utilizzare gli *smart contract* soltanto in maniera ancillare, per l'esecuzione di alcuni profili specifici[425]. L'integrazione fra *smart contract* e *machine learning*, che auspicabilmente avverrà sempre più di frequente nei prossimi anni, lascia sperare in una futura semplificazione della "traduzione" del linguaggio umano in codice[426]. A tutto ciò si aggiunga il fatto che la creazione di uno *smart contract* non può prescindere dal coinvolgimento di un tecnico che sia in grado di traslare in codice la volontà delle parti.

Torna così in gioco un soggetto terzo su cui le parti devono fare affidamento per la conclusione del contratto, sebbene la principale pretesa di questa nuova tecnologia sia proprio quella di eliminare ogni forma di intermediazione. Inoltre, raramente le parti saranno in grado di verificare il grado di accuratezza con cui è stato creato il protocollo e non è difficile immaginare che un tecnico possa snellire il contenuto del contratto per renderne l'esecuzione più veloce ed efficiente, senza contare il fatto che questo processo incide significativamente sui costi da sostenere nella fase esecutiva.

2.3.2. Il trattamento dei dati personali mediante decisioni automatizzate

In linea generale, gli *smart contract* inviano e ricevono dati, che possono essere suddivisi e raccolti in diverse categorie[427]. Vi sono dati irrilevanti da un punto di vista giuridico ed altri soggetti invece all'applicazione di discipline specifiche, quali quella sulla proprietà intellettuale o sulla protezione dei dati personali. In alcuni casi i dati possono rappresentare di per sé una proprietà virtuale, come accade nel caso delle criptovalute.

[425] Levi Stuart, Lipton, (n. 414)
[426] Mik, (n. 412), 287 ss.
[427] Ibid,106 ss.

Per quanto concerne nello specifico i problemi legati alla tutela dei dati personali, possono qui essere richiamate le considerazioni già svolte in relazione alla *blockchain*. E' bene però approfondire il profilo riguardante l'applicazione dell'art. 22 GDPR relativo alle decisioni automatizzate. Non è chiaro infatti se gli *smart contract* possano essere qualificati come tali e se, dunque, la disciplina dettata dal GDPR si applichi o meno a questi ultimi. Si è già avuto modo di vedere che l'art. 22 attribuisce all'interessato il diritto a non essere soggetto a decisioni assunte esclusivamente sulla base di un trattamento automatizzato, senza che vi sia alcun intervento umano. Posto che gli *smart contract* si caratterizzano proprio per il fatto che la loro esecuzione avviene in maniera automatica, occorre capire se questi siano qualificabili come decisioni[428]. Alla luce dell'interpretazione estensiva adottata dalla CGUE, dovrebbe concludersi che almeno in quelle ipotesi in cui attraverso uno *smart contract* si giunge ad un esito al quale si sarebbe comunque giunti con un meccanismo ordinario, cioè anche in presenza di un intervento umano, questo costituisca una decisione ai sensi dell'art. 22 GDPR.

La medesima conclusione sarebbe valida nel caso in cui uno *smart contract* sia utilizzato per dare esecuzione ad obblighi sanciti dalla legge. La prospettiva cambia però a seconda del momento in cui si considera assunta la decisione. Se si ritiene che questa abbia luogo nel momento in cui viene data esecuzione al contratto, non vi sono dubbi sul fatto che manchi ogni tipo di intervento umano.

Anticipando l'analisi ad un momento precedente, questo potrebbe però rilevarsi non più vero, perché uno *smart contract* nasce comunque dal previo accordo fra due o più parti, che stabiliscono esattamente a quali condizioni dovranno prodursi determinati effetti. Secondo una diversa interpretazione, questo potrebbe rilevare ai sensi del comma 2, che esclude l'applicazione della prima parte della disposizione quando la decisione automatizzata è necessaria per l'esecuzione di un contratto. Non pone invece particolari problemi il fatto che ai fini dell'applicazione del comma 1 è necessario che la decisione produca effetti legali o comunque significativi per l'interessato, poiché in linea di massima le conseguenze prodotte dall'esecuzione di uno *smart contract* rientreranno nell'una o nell'altra nozione.

Tornando alle eccezioni stabilite dal comma 2, sorgono dei problemi interpretativi in quanto la lett. a) richiede che il contratto per la cui esecuzione è necessario assumere una decisione automatizzata debba essere concluso fra l'interessato e il titolare del trattamento. Le incertezze sulla ripartizione dei ruoli delineati dal GDPR si ripercuote inevitabilmente sull'applicabilità di questa disciplina. Incertezza vi è anche sulla possibilità di definire necessario il trattamento in esame. La lett. c) del medesimo comma stabilisce inoltre l'inapplicabilità della disposizione nel caso in cui il trattamento sia basato sul consenso esplicito dell'interessato. Fanno qui eco i problemi legati alla validità della base giuridica. Il terzo comma dell'articolo dispone infine che nelle ipotesi in cui operino le eccezioni di cui al secondo comma,

[428] Michele Finck, "Smart Contracts as a Form of Solely Automated Processing Under the GDPR", (2019), vol. 9 no. 2 *International Data Privacy Law*, 83 ss, accessibile da https://academic.oup.com/idpl/article/9/2/78/5488488.

l'interessato ha il diritto di ottenere quantomeno l'intervento umano. Applicando questa previsione nel contesto degli *smart contract*, sorgono tre dubbi fondamentali: cosa s'intende per intervento umano, in quale fase questo dev'essere garantito e, infine, se possa effettivamente essere garantito dal titolare del trattamento.

Ai primi due interrogativi può rispondersi richiamando le linee-guida del Art. 29 WP[429], secondo cui l'intervento richiesto dev'essere tale da poter influire concretamente sulla decisione e può essere anche successivo al momento in cui questa viene assunta. Nel caso degli *smart contract*, dunque, si potrà intervenire anche dopo che il contratto abbia avuto esecuzione. Sebbene questo sia tecnicamente possibile, è comunque difficile nella pratica. Per l'ultimo punto, valgono ancora una volta le considerazioni sulla difficoltà nell'individuare chi figuri come titolare. Si auspica che l'evoluzione della tecnologia e lo sviluppo consentano di creare nuovi modelli di *smart contract*, in grado di conciliarsi più facilmente con le istanze poste dal GDPR.

CAPITOLO III

3. Blockchain-based IoT systems: sfide ed opportunità nell'integrazione fra le due tecnologie.

A conclusione dell'analisi sin qui svolta e sulla scorta delle premesse elaborate, l'obiettivo che ci si propone di raggiungere in questo capitolo è quello di dimostrare in che modo attraverso l'utilizzo della *blockchain* e degli *smart contract* congiuntamente ai sistemi IoT, sia possibile superare le criticità poste da questi ultimi in termini di tutela dei dati personali, evidenziando al contempo gli effetti positivi sulla concorrenza. In altre parole, lo scopo è dimostrare che integrando tecnologie diverse non soltanto se ne ottimizzano le prestazioni, ma ciò consente al tempo stesso di intervenire già a livello strutturale al fine di garantire il rispetto della disciplina.

Alla luce della decisione Facebook Germany (B6-22/16)[430], con la quale il *Bundeskartellamt* tedesco è giunto ad affermare che la violazione della disciplina del GDPR può determinare a certe condizioni una contestuale violazione della disciplina concorrenziale, è ragionevole affermare che lo sviluppo di sistemi

[429] Art. 29 WP, "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679", (n. 159).
[430] Vedi Capitolo I, para 1.3.

in grado di garantire *by-design* il pieno rispetto della normativa sulla tutela dei dati personali, possa al contempo contribuire alla salvaguardia della concorrenza nel mercato interno. Nel corso dell'indagine qui svolta, si è inoltre avuto modo di evidenziare che le più recenti proposte della Commissione per la regolamentazione dei mercati digitali mutuano dalla disciplina del GDPR alcuni importanti elementi, primo fra tutti il diritto alla portabilità dei dati. Anche in questo senso, dunque, può dirsi che un intervento anticipato alla fase di progettazione e sviluppo dei sistemi, con l'introduzione di soluzioni tecniche in grado di garantire il rispetto della disciplina sulla tutela dei dati personali, si concilia con il rispetto della disciplina sulla concorrenza.

E' dunque in quest'ottica che si procederà all'illustrazione delle principali soluzioni tecniche già avanzate in questo settore.

3.1 IoT, blockchain e smart contract: la compatibilità con il GDPR e l'impatto sulla concorrenza

Al fine di dimostrare che l'utilizzo integrato di *blockchain*, *smart contract* e IoT può concretamente contribuire a garantire livelli di *compliance* più alti rispetto alla disciplina di tutela dei dati, verranno dunque analizzati i progetti già esistenti e più rilevanti in questo contesto. Può comunque dirsi sin da questo momento che non si tratta di soluzioni a carattere assoluto, ma l'efficacia di ciascuna di esse è legata al contesto specifico nella quale le si intende utilizzare. Alla luce di questa considerazione, deve dirsi che non potrà comunque prescindersi da un'analisi condotta caso per caso al fine di determinare in concreto quale sarà l'impatto dell'introduzione di un sistema innovativo tanto sui dati personali quanto sulla concorrenza nel mercato.

A. L'identificazione del soggetto

Si è messo in luce che le prestazioni dei sistemi IoT beneficiano (o meglio, dipendono) dall'elaborazione e l'analisi di enormi quantità di dati ma che, al tempo stesso, questo determina la possibilità di identificare più facilmente il soggetto al quale i dati sono riferiti, dilatando la nozione di dato personale e generando incertezze circa l'applicabilità o meno della disciplina dettata dal GDPR. Per ridurre i rischi legati a questo fenomeno, viene incoraggiato l'utilizzo di tecniche di anonimizzazione e pseudonimizzazione dei dati[431].

Una delle possibili integrazioni fra IoT e *blockchain* si focalizza proprio sul miglioramento delle tecniche di pseudonimizzazione dei dati. Una delle soluzioni proposte è quella di dividere i dati personali,

[431] Si ricorda che i dati vengono considerati anonimi se la re-identificazione del soggetto interessato non è più possibile in modo irreversibile. In tal caso questi non sono più dati personali, e l'applicazione del GDPR è esclusa. Al contrario, i dati pseudonimi rimangono comunque personali, dal momento che la re-identificazione non è impossibile, ma solo più difficile.

distribuendoli attraverso i vari dispositivi che compongono un sistema *"smart"* (esempi tipici sono quelli di *smart home* e *smart city*)[432]. In questo modo soltanto chi possiede tali dispositivi è in grado, incrociando i diversi dati, di identificare il soggetto interessato. Quest'ultimo avrà anche il potere di gestire il sistema di accesso ai dati, subordinandolo all'ottenimento di specifiche autorizzazioni.

In generale, molte delle soluzioni proposte si basano su specifici sistemi di autorizzazione[433], sfruttando dunque prevalentemente le *blockchain* di tipo *permissioned*. Si è notato che i tradizionali sistemi di autenticazione non possono essere facilmente implementati nel contesto di sistemi IoT perché ideati avendo in mente un modello di tipo centralizzato. Questa è la ragione per cui i nuovi modelli proposti sfruttano la tecnologia *blockchain*, prevedendo ad esempio che sia uno *smart contract* a contenere le istruzioni per verificare se un determinato soggetto possegga o meno i requisiti necessari per ottenere l'accesso ai dati. Una soluzione elaborata avendo riguardo in modo specifico del contesto di una *smart home*[434], in cui un attacco da parte di un hacker potrebbe condurre non soltanto ad un indebito sfruttamento dei dati personali, ma anche ad un'intrusione fisica nell'appartamento, è quella di introdurre un sistema di autenticazione a due fattori, in cui il secondo *step* di autorizzazione si basa sulla posizione del soggetto che tenta di accedere al dispositivo. In poche parole, se quest'ultimo si trova al di fuori dell'appartamento, l'accesso viene negato e il tentativo registrato su *blockchain*.

Con particolare riguardo dei dati relativi alla salute, ricompresi fra le categorie speciali di dati soggetti alla disciplina di cui all'art. 9 del GDPR, è stato suggerito in particolare l'utilizzo della criptazione, al fine di limitarne l'accesso ai soli soggetti legittimati al loro trattamento e soltanto in presenza delle condizioni opportune. Il riferimento è ai dati rilevati mediante ai dispositivi *"wearable"*, in grado di registrare ad esempio la pressione sanguigna o la temperatura corporea, e che potrebbero trovare utilmente impiego anche all'interno delle strutture ospedaliere. Attraverso un sistema di chiavi criptate basato su *blockchain*, verrebbe data la possibilità ai pazienti di decidere in maniera consapevole e specifica a disposizione di chi mettere la chiave necessaria per la decriptazione dei dati (e dunque l'identificazione del soggetto), mentre i dati in forma aggregata, ma comunque criptati, potrebbero essere utilizzati a fini statistici[435]. Fra i modelli proposti e che intendono sfruttare la criptazione dei dati insieme alla creazione di un meccanismo di accesso differenziato agli stessi, soggetto al pieno controllo da parte dell'interessato, ve ne sono alcuni che prevedono addirittura che decriptazione dei dati venga consentita

[432] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo e Antonio Puliafito, "Blockchain and Iot Integration: A Systematic Survey" (2018), vol.18 no. 8, *Sensors (Basel, Switzerland)*, 2575, accessibile da https://www.mdpi.com/1424-8220/18/8/2575.
[433] Ibid.
[434] Ibid.
[435] Muneeb Ul Hassan, Mubashir Husain Rehmani e Jinjun Chen, "Privacy Preservation in Blockchain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions", 2019, vol. 97 *Future Generation Computer Systems*, 521, accessibile da https://www.sciencedirect.com/science/article/pii/S0167739X18326542?via%3Dihub.

previo pagamento di una somma di denaro[436]. Questo consentirebbe all'interessato di trarre profitto dallo sfruttamento dei propri dati personali e sembra conciliarsi bene con la proposta avanzata dalla Commissione[437] di equiparare i dati personali alla valuta, riconoscendoli come mezzo di pagamento.

Sistemi differenziati di accesso ai dati potrebbero altresì essere predisposti mediante la creazione di *smart contract* che, traducendo in formule matematiche le condizioni richieste dal GDPR per il trattamento dei dati (con particolare riguardo delle categorie speciali di dati di cui all'art. 9), ne garantiscano l'esecuzione[438].

Un'altra soluzione interessante sotto questo profilo è stata proposta per il settore assicurativo con la piattaforma "Aigang"[439], in cui grazie ai dati forniti dai dispositivi IoT è possibile non soltanto avere a disposizione dati più certi per il calcolo del rischio, ma anche eseguire automaticamente i pagamenti dovuti a seguito di un sinistro. Per far fronte ai principali aspetti negativi di questa soluzione, che risiedono principalmente nel fatto che la qualità dei dati prodotti e trasmessi dai dispositivi IoT non è sempre garantita e la loro affidabilità rimane comunque limitata e che, inoltre, l'eccessiva quantità di dati immessi potrebbe compromettere la corretta esecuzione del contratto, sono infatti state ideate soluzioni innovative volte non soltanto a consentire una verifica della correttezza dei dati e dell'affidabilità della fonte, ma anche ad impedire al contempo l'identificazione di quest'ultima. Anche in questo caso la soluzione consiste nella creazione di un sistema di *smart contract* che utilizzando la tecnologia *zero-knowledge proof*[440] permette di redigere il contratto in modo tale che questo sia in grado di selezionare gli elementi rilevanti per valutare la correttezza, senza però distribuire sulla catena i dati personali che potrebbero esservi contenuti.

---

[436] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, e altri, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey", 2019, vol. 21 no. 2 *IEEE Communications Surveys and Tutorials*, 1690, accessibile da https://s3-us-west-2.amazonaws.com/ieeeshutpages/xplore/xplore-ie-notice.html.

[437] Commissione, Proposta per una Direttiva del Parlamento europeo e del Consiglio su certi aspetti concernenti i contratti per la fornitura di servizi digitali, (n. 119).

[438] Masoud Barati, Ioan Petri e Omer Rana, "Developing GDPR Compliant User Data Policies for Internet of Things", (2019) *Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing,* , 138-139, accessibile da https://dl.acm.org/doi/10.1145/3344341.3368812.

[439] Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler e Manuel Díaz. "On Blockchain and its Integration with IoT. Challenges and Opportunities", 2018, vol. 88 *Future Generation Computer Systems*, 179, accessibile da https://www.sciencedirect.com/science/article/pii/S0167739X17329205?via%3Dihub.

[440] La tecnologia *zero-knowledge proof* è caratterizzata dal fatto che consente a chi la utilizza di dimostrare un determinato assunto, senza fornire però informazioni ulteriori rispetto a quelle desumibili da quest'ultimo. (Per una trattazione completa del tema si veda Shafi Goldwasser, Silvio Micali e Chiarles Rackoff, "The knowledge complexity of interactive proof systems", (1989), Vol 18, No. 1 *Society for Industrial and Applied Mathematics*, pp. 186-208, accessibile da https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf). Sfruttando queste caratteristiche per dare esecuzione ad uno *smart contract*, è pertanto possibile dimostrare che si siano verificate le condizioni necessarie per attivare il contratto, senza però comunicare elementi ulteriori, con un evidente impatto positivo in termini di tutela dei dati.

Uno dei progetti che viene più spesso citato come esempio di sistema basato su *smart contract* e funzionale alla tutela dei dati personali è "Hawk"[441], sviluppato da alcuni studiosi dell'Università del Maryland e della Cornell University. Tale sistema nasce dall'esigenza di tutelare i soggetti che eseguono transazioni su *blockchain*, evitando che i dati transazionali riferiti a queste ultime vengano caricati direttamente sulla catena e siano di conseguenza visibili a tutti. Ad essere presente e visibile sulla catena sarà dunque la traccia dell'operazione, ma non ad esempio i dati relativi alla quantità di denaro trasferita, protetti invece dalla criptografia. L'esecuzione del contratto può essere facilitata dalla presenza di un soggetto terzo detto *manager*, ma a differenza di quanto avviene nei sistemi ordinari, questo non potrà in alcun modo impedire l'esecuzione del contatto e qualora dovesse violare il protocollo scelto, le parti maturerebbero il diritto ad un compenso per la perdita subìta.

Nel contesto dei progetti di integrazione fra i sistemi IoT e la tecnologia degli *smart contract*, particolare attenzione merita il progetto DECODE[442], finanziato nell'ambito del programma "Horizon2020" promosso dall'Unione Europea. Il progetto nasce proprio con il fine di sviluppare soluzioni innovative volte a fornire nuovi servizi ai cittadini, restituendo loro il pieno controllo sui propri dati personali.

Il gruppo di ricercatori e *start-uppers* che se ne occupa ha puntato principalmente su due progetti pilota, rispettivamente nelle città di Barcellona e Amsterdam. Al progetto è stata data vita nel 2018, e da allora i risultati raggiunti sono notevoli. Nell'illustrare quelli più significativi, ci si soffermerà nello specifico sulle iniziative intraprese nella città spagnola, ed in particolare sui progetti CitizenSensing (IoT)[443] e Digital Democracy and Data Commons (da qui in poi "DDDC")[444].

Sia nell'uno che nell'altro caso viene in rilievo il trattamento dati personali, che variano da quelli legati alla posizione geografica ai dati anagrafici. Vi rientrano in certi casi anche le categorie speciali di dati ai sensi dell'art. 9 del Regolamento (UE) 2016/679, poiché le informazioni richieste agli utenti che intendono accedere al servizio ne rivelano l'orientamento politico, l'origine razziale e altri fra gli elementi rilevanti per la disciplina del GDPR. Gli sviluppatori del progetto si sono dunque soffermati sull'analisi delle criticità legate al trattamento dei dati, ipotizzando le soluzioni migliori per porvi rimedio[445]. Entrambi i sistemi sono stati sviluppati prevedendo forme di criptazione dei dati raccolti dagli utenti, ma era evidente che ciò non fosse sufficiente ad arginare i rischi legati alla tutela dei dati

[441] Ahmed Kosba, Andrew Miller, Elaine Shi, et al. "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", (2016), *Proceedings - 2016 IEEE Symposium on Security and Privacy,* accessibile da https://s3-us-west-2.amazonaws.com/ieeeshutpages/xplore/xplore-ie-notice.html.

[442] "DECODE", <https://decodeproject.eu/what-decode> ultimo accesso Maggio 2021.

[443] Si tratta di un progetto finalizzato alla raccolta dati relativi alle condizioni climatiche, alla temperatura, ai livelli di inquinamento acustico e ambientale, attraverso la distribuzione di dispositivi IoT ai cittadini, grazie ai quali viene restituito loro un quadro continuamente aggiornato della situazione nelle varie aree della città.

[444] Si tratta un servizio che consente ai cittadini di firmare delle petizioni collettive. La procedura prevede una prima fase in cui, per potere accedere al servizio, gli utenti devono fornire i propri dati demografici e possono autorizzare l'utilizzo degli stessi a fini statistici.

[445] "Privacy Strategies for de DECODE architecture", (2019), accessibile da https://decodeproject.eu/publications/privacy-design-strategies-decode-architecture-0.

personali, dal momento che dati provenienti da dispositivi diversi sono messi fra loro in correlazione nella fase di cosiddetta "integrazione", riproponendo il problema di re-identificazione del soggetto interessato. Allo stesso tempo, gli sviluppatori hanno valutato i rischi legati all'utilizzo delle informazioni di cui dispongono i *data miners* che spesso gestiscono *databases* in cui è raccolta un'immensa mole di dati. La soluzione proposta è quella di sviluppare, in ossequio al principio di *privacy-by-design* sancito dal GDPR, soluzioni tecniche che affianchino e rendano concretamente possibile l'attuazione delle disposizioni legislative. Fra quelle individuate figurano proprio la tecnologia *blockchain* e gli *smart contract*.

Alla prima, descritta come un registro aperto in grado di dar vita ad una rete decentralizzata utile alla conservazione dei dati in forma criptata, viene riconosciuto il vantaggio di poter consentire lo sviluppo di un sistema di *mining* più sicuro e controllato. Per quanto riguarda invece gli *smart contract*, questi potrebbero trovare due diverse applicazioni. Da un lato, consentirebbero agli utenti l'esercizio dei propri diritti *"by design"*, cioè integrando direttamente le disposizioni del GDPR. A questa prima funzione se ne accompagnerebbe una seconda, consistente nell'utilizzo di specifici contratti ispirati alla logica generale di *business* e utilizzati per verificare la validità degli accordi fra i singoli utenti, senza però avere accesso alle informazioni specifiche di quell'accordo.

Una volta individuati gli *smart contract* come possibile soluzione ai rischi concernenti la tutela dei dati, gli sviluppatori del progetto DECODE hanno portato avanti la propria indagine, sviluppando un modello di contratto compatibile con la disciplina del GDPR. Da questo studio è nato "Zenroom", un particolare *smart contract* la cui efficacia è stata testata sia nell'ambito del progetto CitizenSensing (IoT) che DDDC.

Il report del progetto[446] evidenzia proprio il fatto che la struttura e le funzioni specifiche del contratto variano a seconda dell'applicazione concreta che deve farsene, non potendo immaginare soluzioni valide in modo assoluto. In queste ipotesi, il contratto è stato utilizzato sia per consentire un processo di autenticazione anonima degli utenti, in linea con il principio di *privacy-by-default* sancito dal GDPR, sia per la criptazione di dati di natura diversa. Solo nel caso del progetto DDDC, invece, il contratto era deputato anche alla gestione dell'intero procedimento di creazione e sottoscrizione della petizione, per consentire che il voto espresso da ciascun partecipante venisse registrato sulla catena in forma criptata ed identificato attraverso una serie casuale di numeri, anche stavolta in ossequio al principio di *privacy-by-default*.

Nell'ambito del progetto DECODE, si è tenuto a mettere in risalto un profilo ulteriore, riconducibile alla difficoltà di conciliare sistemi e categorie diverse fra loro, al fine di costruire un codice universalmente

[446] "Smart contracts for data commons", (2019), accessibile da https://decodeproject.eu/publications/smart-contracts-data-commons.

condivisibile[447]. Si è più volte ribadito che le tecnologie di cui si sta qui trattando non conoscono confini geografici e legare il loro funzionamento ad un ordinamento giuridico specifico ne ridurrebbe la potenzialità, ostacolando l'interoperabilità fra sistemi diversi. Occorre dunque favorire lo sviluppo di un vocabolario comune, di regole uniformi per verificare la *compliance* dei contratti rispetto alla legislazione, di sistemi di interfaccia che facilitino la comprensione degli *smart contract* da parte degli utenti, nonché dell'utilizzo degli "oracoli" al fine di garantire l'adattamento dei suddetti sistemi al cambiamento delle circostanze[448].

B. I principi e diritti dell'interessato

Il principio di liceità e le basi giuridiche del trattamento

Gli *smart contracts* basati su *blockchain* potrebbero essere utilizzati per determinare a priori le regole che i dispositivi che compongono i sistemi IoT dovranno seguire nell'esecuzione delle varie transazioni. Per quello che qui interessa, tali strumenti potrebbero contribuire a risolvere uno dei problemi più rilevanti posti dallo sviluppo delle nuove tecnologie, ossia l'individuazione di una corretta base giuridica che legittimi il trattamento dei dati personali, in ossequio al principio di liceità sancito dall'art. 5 del GDPR.

Oggetto dello *smart contract* potrebbe infatti essere l'ottenimento da parte dell'interessato del consenso al trattamento dei propri dati personali ("*user consent contract*")[449], una volta che ne sia stata accertata la legittimità mediante l'attivazione di un altro *smart contract* ("*GDPR-compliance contract*") di cui è responsabile il titolare del trattamento. In questo modo si vuole risolvere il problema di asimmetria informativa ed incertezza evidenziato nei capitoli precedenti e che ha fatto sorgere dubbi sulla validità del consenso quale base giuridica. Il soggetto interessato ha infatti la garanzia che il trattamento rispetta la disciplina del GDPR, in quanto ciò costituisce una delle condizioni necessarie perché possa essere data attuazione al primo dei due contratti. Inoltre, l'attivazione del contratto specificatamente posto alla prestazione del consenso dell'interessato è comunque rimessa alla scelta di quest'ultimo (consenso libero). Il modello proposto si compone di almeno altri due *smart contract* funzionali ad evitare eventuali

[447] "Legal ontology to support contracts in DECODE scenarios", accessibile da https://decodeproject.eu/publications/decode-legal-ontology-smart-contracts.

[448] Ibid. Il modello che viene proposto è articolato su diversi livelli e si compone di vari *step* attuativi. Anzitutto, sono necessari input provenienti da norme, casi giurisprudenziali e contratti, al fine di trarre da tutte queste fonti i concetti più rilevanti. Questi vengono dunque analizzati, per poi essere catalogati e distinti sulla base del valore semantico corretto da attribuire a tutti i termini ivi contenuti, tenendo conto anche della possibilità che alcuni di essi possano assumere vari significati. I concetti così catalogati vengono allora ricondotti ad un determinato ordinamento, in modo tale da consentire sia l'individuazione di figure specifiche (ad esempio, sulla base dei dati inseriti sarà possibile determinare chi è qualificabile come titolare del trattamento), sia l'utilizzo corretto dello *smart contract* nel contesto concreto. Chiaramente ciò diviene tanto più complesso quanto maggiori siano le differenze fra gli ordinamenti tenuti in considerazione. Il successo di questa tecnica dipenderà dunque anche dalla capacità di elaborare, nella misura in cui ciò è possibile, un sistema di norme comuni.

[449] Barati, Petri e Rana, (n. 438), 138-139.

violazioni successive alla fase iniziale del trattamento, consistenti ad esempio nella raccolta di dati ulteriori rispetto a quelli originariamente comunicati all'interessato e/o al perseguimento di altre finalità. Il primo dei due contratti (*"submission contract"*) presuppone che il titolare registri e carichi su *blockchain* tutte le operazioni eseguite sui dati personali dell'interessato. Il secondo ("*verification contract"*) provvederà invece a verificare, ed eventualmente segnalare, se le attività registrate si discostino in qualche modo dalle condizioni originariamente pattuite e contenute nel *GDPR-compliance contract*.

Un'altra soluzione ispirata al medesimo scopo prevede invece l'utilizzo della *blockchain* per impedire che uno dei dispositivi che compongono il sistema IoT possa essere attivato e possa accedere ai dati personali dell'utente qualora quest'ultimo non abbia previamente accettato le *privacy policy* che regolano l'utilizzo dei dati personali[450]. Anche in questo caso è previsto l'impiego di *smart contract*, per consentire all'utente di avere contezza di quali siano i dispositivi collegati alla *blockchain* e di scegliere se accettare o meno le condizioni previste da ciascuno di essi.

Il principio di trasparenza

La trasparenza nel trattamento dei dati, difficile da garantire nei sistemi IoT in ragione delle tecniche di analisi algoritmica generalmente impiegate, è uno degli aspetti che beneficerebbe maggiormente dell'utilizzo della *blockchain* nei sistemi IoT. La struttura decentralizzata e trasparente della *blockchain*, restituirebbe agli utenti la possibilità di tenere sotto controllo tutte le operazioni di cui sono oggetto i loro dati personali, nonché a verificare la correttezza di questi ultimi[451]. L'utilizzo di una catena comune fra i dispositivi che compongono un sistema permetterebbe inoltre ai soggetti interessati di identificarli più facilmente, acquisendo piena consapevolezza di quali dispositivi utilizzino effettivamente i loro dati e in che modo. Questo è ancora più vero nel caso di *blockchain permissioned*, in cui la partecipazione alla catena è subordinata ad un sistema di autorizzazioni e verifiche in grado di dare maggiore certezza sull'identità e l'affidabilità dei dispositivi coinvolti.

Principio di minimizzazione dei dati

Tenuto conto tanto delle caratteristiche proprie dei sistemi IoT, quanto di quelle della *blockchain*, si è sempre dubitato dell'effettiva possibilità di garantire l'attuazione del principio di minimizzazione. L'integrazione nei dispositivi IoT di sistemi filtro in grado di selezionare i dati più utili, cioè quelli dai quali è possibile trarre le informazioni davvero rilevanti ai fini del trattamento, nonché quelli ritenuti

[450] Panarello, Tapas, Merlino, Longo e Puliafito, (n. 432), 27.
[451] Reyna, Martín, Chen, Soler Díaz, (n. 439).

maggiormente affidabili, potrebbe contribuire ad un miglioramento sotto questo profilo[452]. Tali sistemi potrebbero essere gestiti mediante *smart contract*, ovviando anche ad un problema ulteriore, generalmente considerato come un ostacolo all'integrazione delle due tecnologie: l'effettiva capacità della *blockchain* di conservare le enormi quantità di dati prodotte dai sistemi IoT. Se la catena non fosse in grado di contenere tutti i dati prodotti all'interno di questi sistemi, infatti, la loro funzionalità ne risulterebbe particolarmente compromessa.

Principio di esattezza

Si è già detto che i dispositivi che compongono i sistemi IoT potrebbero essere utilizzati nella funzione di "oracoli" degli *smart contract*, ossia come fonti da cui tali contratti traggono i dati loro necessari per dare esecuzione alle clausole ivi previste. Nonostante l'incredibile potenzialità di questa soluzione, che consentirebbe agli *smart contract* di avere la disponibilità di tutti i dati necessari alla loro attivazione, creando un meccanismo di gestione dei dati che circolano all'interno dei sistemi IoT, potrebbero porsi dei problemi riguardanti l'esattezza dei dati[453]. Il contratto, infatti, non è in grado di verificare se i dati immessi nel sistema siano corretti e ciò potrebbe comportare dei rischi per gli utenti. Affinché l'intero meccanismo funzioni correttamente, è dunque necessario che i dispositivi che compongono i sistemi IoT siano previamente soggetti a test e controlli volti ad indagarne eventuali malfunzionamenti, nonché l'esistenza di eventuali componenti esterne o attacchi, che possano compromettere la qualità dei dati da essi trattati[454].

Principio di limitazione della conservazione dei dati e diritto alla cancellazione

La conservazione dei dati per un periodo limitato, nonché il concreto esercizio del diritto di cancellazione di cui all'art. 17 del GDPR, possono essere garantiti attraverso la creazione di *smart contract* che traducano in codice la normativa. In questo modo è possibile verificarne il rispetto prima che il trattamento dei dati abbia effettivamente inizio, garantendo che qualora non sussistano le condizioni necessarie, questo non abbia luogo. In altre parole, le questioni legali rilevanti per il GDPR vengono inserite nel contratto in forma di "domande" tradotte in codice. Tenendo presenti le difficoltà già analizzate nella traslazione di concetti giuridici in formule matematiche, porre in essere una soluzione di questo genere potrebbe rivelarsi utile in circostanze specifiche, ossia in relazione a disposizioni che si prestano a questo genere di meccanismo. Quanto al periodo di conservazione dei dati, ad esempio, dal momento che l'intervallo di tempo necessario per il trattamento è un valore definito, questo può

[452] Ibid.
[453] Ibid.
[454] Ibid.

facilmente essere traslato in formula ed inserito nello *smart contract*[455]. Allo stesso modo, il contratto potrà contenere l'indicazione relativa al potere riconosciuto all'utente (cioè al soggetto interessato) di cancellare alcuni dati conservati, in ossequio a quanto stabilito dalla disciplina.

Principio di sicurezza

La sicurezza dei sistemi IoT è uno degli elementi che desta maggiori preoccupazioni, dal momento che i dispositivi potrebbero facilmente essere soggetti ad attacchi che causerebbero la distruzione dei dati o il loro trattamento illecito. Accrescere i livelli di sicurezza è dunque una priorità assoluta e contribuirebbe al rafforzamento della fiducia in questi sistemi, favorendone la diffusione. Sotto questo profilo, l'utilizzo della *blockchain* è una delle soluzioni a cui si guarda con maggior favore, perché le caratteristiche proprie di quest'ultima si sposano benissimo con i problemi sollevati dai sistemi IoT. In primo luogo, sostituendo un sistema *peer-to-peer* alla tradizionale architettura centralizzata di gestione dei sistemi, non vi sarebbe più un singolo *point-of-failure*, ossia un punto vulnerabile agli attacchi, garantendo maggiore sicurezza[456].

Un altro aspetto rilevante dal punto di vista della sicurezza concerne invece le comunicazioni fra i vari dispositivi. Anche queste, infatti, possono essere oggetto di attacchi e possono far venir meno quel carattere di integrità dei dati personali soggetti a trattamento, che ai sensi del GDPR dev'essere invece garantito. Per migliorare i livelli di sicurezza sotto questo profilo, le comunicazioni fra i dispositivi IoT potrebbero essere registrate su *blockchain* come transazioni della catene e validate tramite *smart contract*[457]. In tal modo non solo si potrebbe verificare la correttezza delle comunicazioni, ma anche di impedire l'alterazione dei dati in conseguenza di un attacco al sistema. Più in generale, le tecniche di criptazione dei dati normalmente utilizzate dalla *blockchain* possono essere utilizzate, oltre che al fine di impedire la re-identificazione dell'interessato, anche per migliorare i livelli di sicurezza delle comunicazioni[458].

Principio di responsabilità

Il titolare del trattamento potrebbe beneficiare dell'utilizzo della *blockchain* per rispondere degli obblighi che gravano su di lui ai sensi della disciplina sulla tutela dei dati personali. Attraverso l'attivazione di uno specifico *smart contract*, infatti, quest'ultimo potrebbe registrare tutti gli elementi

[455] Baratri, Petri, Rana, (n. 421), 137-138.
[456] Reyna, Martín, Chen, Soler e Díaz, (n. 439), 179.
[457] Ibid, 181.
[458] Ibid, 182.

relativi al trattamento dei dati personali e le attività concretamente svolte su di essi[459]. Caricando queste informazioni su *blockchain*, se ne garantirebbe l'immutabilità e l'assoluta trasparenza, consentendo al titolare di dimostrare molto più facilmente di avere eseguito il trattamento nel rispetto di tutti i principi dettati dal GDPR.

C. Privacy-by-design e privacy-by-default

Da ultimo, è bene ricordare che una delle novità più importanti introdotte dal GDPR e finalizzate a garantire l'effettiva attuazione delle norme ivi contenute, alla luce della necessità di favorire l'adozione di un approccio *"zero-risk"*, che, cioè, minimizzasse il rischio di danni per i dati personali degli individui, è rappresentata proprio dai principi di *privacy-by-design* e *privacy-by-default*. Come si è già ampiamente avuto modo di illustrare, tali principi tendono ad incoraggiare l'adozione di misure tecniche ed organizzative che garantiscano il rispetto della normativa, intervenendo già nella fase di progettazione. Vi si includono tutte le misure idonee a restituire un maggior controllo sui dati all'interessato, ivi compresi i meccanismi di controllo sull'accesso ai dati, basati su sistemi di autorizzazioni differenziate[460] ai quali, come si è visto, si può dar vita mediante l'utilizzo diversi *smart contract*. Quanto qui si propone, ossia di migliorare i livelli di *compliance* grazie al loro utilizzo integrato con la tecnologia *blockchain* e gli *smart contract*, si pone dunque perfettamente in linea con l'approccio auspicato dalla disciplina UE, nonché con i cosiddetti "principi fondanti" del concetto di *privacy-by-design*[461].

In primo luogo, infatti, l'approccio qui suggerito è di carattere proattivo e preventivo, e non reattivo e rimediale[462]. Lo scopo ultimo al quale si tende è quello di favorire la nascita di una nuova generazione di sistemi IoT strutturalmente idonei a garantire il rispetto della disciplina sulla tutela dei dati. Non è dunque necessario che l'interessato assuma un atteggiamento attivo o compia attività specifiche perché sia garantita la piena tutela dei suoi dati personali, in quanto è il dispositivo stesso, in virtù del suo meccanismo di funzionamento, che lo assicura in tal senso. Questo concetto è particolarmente rilevante nel contesto delle nuove tecnologie, caratterizzato dalla forte asimmetria fra le parti e dall'incapacità o forte difficoltà nel fornire all'interessato tutte le informazioni necessarie. Pensare a soluzioni future grazie alle quali quest'ultimo possa fare affidamento sulla tecnologia stessa per avere certezza che la tutela dei propri dati personali è comunque garantita, contribuirebbe quantomeno a ridurre i problemi derivanti dal gap informativo. Questo si ricollega al fatto che grazie alla *blockchain* e agli *smart contract* le parti coinvolte non hanno bisogno di riporre la propria fiducia le une nelle altre, né in un ente

[459] Baratri, Petri, Rana, (n. 421), 138.
[460] Ali, Vecchio, Pincheira, (n. 439).
[461] Cavoukian, (n. 198).
[462] Ibid.

centralizzato e responsabile per garantire il rispetto della disciplina, ma potranno fare affidamento nella tecnologia stessa e nelle caratteristiche ad essa intrinseche.

Un altro importante elemento che figura fra i principi fondanti del concetto di *privacy-by-design* è l'idea che le soluzioni proposte debbano essere ispirate ad un approccio *win-win*, nel senso che queste siano in grado di garantire contestualmente il rispetto di diversi principi[463]. Il tipico esempio in questo senso è dato dal rapporto fra la tutela dei dati e la sicurezza, poiché si ritiene che garantendo l'una debba essere sacrificata l'altra. Secondo quanto si è qui messo in luce, grazie all'utilizzo della *blockchain* si otterrebbe il risultato diametralmente opposto, poiché una delle principali caratteristiche di tale tecnologia è rappresentata proprio dal suo altissimo livello di sicurezza, e proprio per tale ragione l'ENISA ne incoraggia l'utilizzo integrato ai sistemi IoT. Più in generale, viene sottolineato che le soluzioni *privacy-by-design* non debbano compromettere le prestazioni dei sistemi. Anche in questo caso, si è visto che, al contrario, l'integrazione fra IoT, *blockchain* e *smart contract*, è anzi auspicabile proprio perché permetterebbe a ciascuna di esse di migliorare le proprie prestazioni.

Il sesto dei principi fondanti della *privacy-by-design*[464] fa riferimento alla visibilità e alla trasparenza. Tale principio mira ad assicurare che tutti i soggetti che operano sul mercato, a prescindere dalla specifica attività svolta, seguano le stesse regole sulla tutela dei dati personali e siano trasparenti sulle modalità impiegate a tal fine. Questo ha degli effetti positivi sia sui livelli di fiducia degli utenti verso le nuove tecnologie, sia in quanto comporta un maggiore senso di responsabilità per i titolari.

Si tratta di uno degli elementi che permette di costruire un ponte fra la tutela dei dati personali e quella della concorrenza, dal momento che il fatto che le imprese siano trasparenti sui mezzi da loro utilizzati al fine di adempiere agli obblighi di tutela dei dati ha l'effetto di scongiurare possibili abusi che possano dar luogo al fenomeno della cosiddetta "concorrenza sulla privacy", consentendo di monitorare più facilmente ciò che accade sul mercato.

Le soluzioni qui proposte si conciliano perfettamente anche con questo profilo, dato che, come si è avuto modo di illustrare, una delle caratteristiche più rilevanti della *blockchain* è data proprio l'assoluta trasparenza della catena.

E. L'impatto sulla concorrenza

Nel procedere con l'analisi dei benefici che l'integrazione fra *blockchain, smart contract* e i sistemi IoT può portare alla concorrenza, occorre tenere presente lo specifico punto di vista dal quale s'intende affrontare la questione. L'indagine sin qui condotta muove infatti da una considerazione precisa, ossia

[463] Ibid.
[464] Ibid.

che nel panorama dell'UE vi è una sempre maggiore convergenza fra la disciplina relativa alla tutela dei dati e quella dettata in materia concorrenziale, come dimostrato dalla recente decisione Facebook Germany (B6-22/16). Questo fenomeno, che trova la propria origine nella consapevolezza del valore economico dei dati e del ruolo giocato da questi elementi nel definire il potere e gli equilibri di mercato, non solo sta conducendo verso il superamento dell'indirizzo giurisprudenziale tradizionale, fermo nel ritenere che l'applicazione dell'una e dell'altra disciplina fosse del tutto distinta, ma è emerge anche dalle più recenti proposte presentate dal legislatore europeo nell'ambito del cosiddetto Digital Market Package[465]. In particolare, dall'analisi di queste ultime emergono due elementi di fondamentale importanza: da un lato, proprio in ragione del fatto che sia stato riconosciuto ai dati il valore di *asset* strategico, s'intende favorirne la circolazione e lo scambio fra le imprese, così che l'accesso ai dati (ivi compresi i dati personali) non si trasformi in barriera all'entrata del mercato, consentendo il rafforzamento della posizione di alcune imprese a scapito di altre; dall'altro, vi è la tendenza a ribaltare l'impostazione della disciplina concorrenziale, favorendo un intervento *ex ante* e di natura preventiva, a scapito dell'attuale meccanismo che opera *ex post* e in via rimediale.

Per facilitare lo scambio e la circolazione dei dati fra le imprese, la Commissione ha mutuato proprio dalla disciplina sulla tutela dei dati personali uno dei diritti più innovativi ed importanti introdotti dal GDPR, ossia il diritto alla portabilità dei dati ex art. 20 del Regolamento (UE) 2016/679.

È già stato messo in luce che tale diritto, molto più degli altri sanciti dal GDPR, nasce con una vocazione fortemente commerciale. Pur nel rispetto della *ratio* generale che sottende l'intera disciplina, che mira ad attribuire all'interessato il pieno controllo sui propri dati personali, al contempo la norma vuole infatti favorire la possibilità per tutte le imprese di avere il medesimo accesso a questi ultimi, incoraggiando l'adozione di soluzioni *privacy-friendly* che le rendano più attraenti rispetto ai propri concorrenti.

La potenzialità economica del diritto alla portabilità, enfatizzata dall'avvento dell'economia *data-driven*, è stata bene intuita dalla Commissione[466], che ne incoraggia il rafforzamento negli sviluppi futuri. Questa si è espressa proprio con riferimento ai sistemi IoT, sottolineando che garantire il facile esercizio del diritto alla portabilità avrebbe un impatto positivo non soltanto sulla tutela dei dati personali, ma anche sulla concorrenza e l'innovazione, scongiurando pratiche illecite e i cosiddetti effetti *lock-in*[467].

[465] Vedi nota 207.

[466] Commissione, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati* (n. 228), 8.

[467] La fiducia nell'impatto che il diritto alla portabilità può avere sul futuro dei mercati e della libera concorrenza nel mercato interno è ulteriormente dimostrato dal fatto che ne viene fatta espressa menzione fra gli obblighi a cui sarebbero soggette le piattaforme (i cosiddetti "gatekeeper") ai sensi dell'art. 6 del Digital Market Act. In primo luogo, la lett. h) el predetto articolo impone ai gatekeeper l'obbligo di garantire l'effettivo esercizio del diritto alla portabilità dei dati da parte degli utenti finali, in ossequio a quanto stabilito dal GDPR. La proposta della Commissione si spinge però oltre, estendendo il diritto ad accedere ed usufruire dei dati – sia in forma aggregata che non – anche ai cosiddetti "utenti business", pur nel rispetto della disciplina sulla tutela dei dati personali. Per quel concerne in particolar modo questi ultimi, il diritto degli utenti business di usufruirne è comunque

Presupposto indefettibile affinché il diritto alla portabilità dei dati trovi piena e concreta attuazione è l'interoperabilità fra i sistemi, cioè la capacità di questi ultimi di comunicare fra loro, anche e soprattutto grazie alla diffusione di standard comuni. Non avrebbe alcun senso, infatti, riconoscere alle altre imprese il diritto di accesso e utilizzo dei dati qualora questi non siano forniti in un formato fruibile per tutti o se le differenze fra i vari sistemi ne rendessero tecnicamente impossibile l'esercizio. La stessa Commissione[468] auspica la diffusione di strumenti appropriati e standard unici, che permettano di estendere l'esercizio di tale diritto a settori ulteriori rispetto a quanto avviene attualmente, sottolineando che questo potrebbe innescare un processo virtuoso in cui gli individui siano incoraggiati a mettere i propri dati personali anche al servizio dell'interesse pubblico (ad esempio per svolgere attività di ricerca nel settore sanitario).

L'interoperabilità fra sistemi diversi, a prescindere dal soggetto che li ha sviluppati[469], è uno dei vantaggi maggiori che potrebbe derivare dall'integrazione fra *blockchain* e sistemi IoT. Infatti, mentre sistemi centralizzati non necessariamente (e, nella prassi, poco probabilmente) sarebbero in grado di comunicare gli uni con gli altri, una struttura decentralizzata basata su *blockchain* e *smart contract* consentirebbe lo scambio di informazioni e l'esecuzione di operazioni anche fra dispositivi o sistemi sviluppati da soggetti diversi, eliminando il rischio di trasferire informazioni commercialmente sensibili a potenziali concorrenti. Questo consentirebbe ai sistemi IoT di adattarsi più facilmente ai diversi contesti nei quali vengono impiegati, migliorandone i livelli di adattabilità e dunque le prestazioni[470]. Da una maggiore interoperabilità fra sistemi e dispositivi deriverebbero infatti vantaggi anche su profili diversi rispetto alla *compliance* con il GDPR o la tutela della concorrenza. Ad esempio, nel settore sanitario questo consentirebbe di facilitare la circolazione dei dati fra strutture e reparti diversi, garantendo una migliore assistenza ai pazienti[471]. Il contesto nel quale il valore dell'interoperabilità può essere apprezzato maggiormente rimane comunque quello delle *smart city*, nelle quali inevitabilmente vi è l'incontro e la necessità di dialogo fra realtà molto diverse le une dalle altre e potrebbero apprezzarsi i risultati migliori[472].

---

subordinato al fatto che l'utilizzo che si intende farne è connesso all'utilizzo che l'utente finale farà dei prodotti o servizi offerti dalla piattaforma e comunque previo consenso dello stesso.

[468] Commissione, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati* (n. 228), 8.

[469] Si veda diffusamente Primavera De Filippi e Aaron Wright, "The future of organization" in Blockchain and the Law: The Rule of Code (2018, Cambridge: Harvard University Press), accessibile da https://www.jstor.org/stable/j.ctv2867sp.

[470] Ali, Vecchio, Pincheira, (n. 439).

[471] Mohammad Jabed, Morshed Chowdhury, Md Sadek Ferdous, Kamanashis Biswas, e al, "A Survey on Blockchain-Based Platforms for IoT use-Cases", (2020), vol. 35, *Knowledge Engineering Review*, 7-9, accessibile da https://www.cambridge.org/core/journals/knowledge-engineering-review/article/survey-on-blockchainbased-platforms-for-iot-usecases/0E0A4C27EEBAA12139E6C80D49C03BF2.

[472] Un progetto interessante in tal senso è quello sviluppato dalla società Filament, che ha proposto di creare un *network wireless* finalizzato a controllare tutti i sistemi presenti all'interno della città, che sarebbero in grado di raccogliere dati, scambiare messaggi e interagire gli uni con gli altri in maniera autonoma e senza necessità di intervento umano, grazie all'utilizzo di *blockchain* e *smart contract.* Ciascun dispositivo è ammesso al sistema previa autenticazione e soltanto se condivide il medesimo protocollo di comunicazione adottato dagli altri. (Panarello, Tapas, Merlino, Longo e Puliafito, (n. 432), 19).

Anzitutto, l'integrazione fra *blockchain* e IoT potrebbe avere un impatto sul modo in cui i dispositivi che compongono i sistemi IoT comunicano fra loro[473]. E' possibile individuare almeno tre diversi modelli: il primo prevede che la comunicazione avvenga esclusivamente fra i dispositivi IoT, limitando l'impiego della *blockchain* alla sola conservazione di alcuni dati; il secondo modello si pone su piano diametralmente opposto, prevedendo cioè che tutte le transazioni siano effettuate sulla catena (*blockchain*) e siano di conseguenza non modificabili; può scegliersi, infine, un modello ibrido, dove soltanto alcune transazioni sono effettuate *on-chain*, mentre le altre avvengono direttamente fra i dispositivi IoT. La scelta dell'uno o dell'altro modello dipenderà essenzialmente dall'utilizzo che se ne dovrà fare.

Se è pur vero che l'attuale disciplina sulla concorrenza riconosce in capo alla Commissione dei poteri di controllo preventivi (è quanto accade, ad esempio, nella disciplina sulle concentrazioni), in via generale questa, alla pari delle autorità nazionali competenti, interviene soltanto quando vi sia ragione di credere che una violazione della disciplina sia già stata commessa. Al contrario, grazie all'introduzione del GDPR il legislatore UE ha favorito l'adozione di un approccio *"zero-risk"*, basato cioè sulla predisposizione di tutte le misure ragionevolmente necessarie a prevenire ogni possibile violazione e danno per l'interessato. La diversa impostazione adottata dall'una e dall'altra disciplina si spiega alla luce dei diversi interessi che queste mirano a tutelare, in quanto, mentre la disciplina concorrenziale mira a proteggere interessi puramente economici, quella sulla tutela dei dati personali ha ad oggetto la tutela dell'individuo. L'utilizzo dei dati nell'economia ha reso sempre più sottile la linea di demarcazione fra l'uno e l'altro aspetto. Dal momento che le tecniche sempre più sofisticate di analisi dei dati hanno enfatizzato il rischio che il trattamento dei dati personali non rispetti le direttive impartite dal GDPR e che questo può tradursi in squilibri per la concorrenza (cosiddetta "competizione sulla privacy"), non soltanto è ragionevole che le violazioni della disciplina sulla tutela dei dati siano rilevanti anche alla luce della normativa sulla concorrenza, ma anche che questa cambi il proprio approccio. Rafforzare meccanismi di intervento preventivi è quindi indispensabile perché le norme poste a tutela del mercato trovino efficacemente applicazione e siano in grado di far fronte alle sfide poste dai nuovi mercati.

A tal fine, intervenire sul piano esclusivamente normativo sarebbe insufficiente, alla pari di quanto si è rivelato esserlo nell'ambito della disciplina sulla tutela dei dati. Anche in questo caso, è dunque auspicabile lo sviluppo di soluzioni tecniche, secondo un approccio che – richiamando il linguaggio adottato dal GDPR – si potrebbe definire come *"competition-by-design"*.

A questo punto occorre riflettere su due diversi temi. Da un lato, se il rispetto della normativa sulla tutela dei dati è esso stesso elemento rilevante per la concorrenza, ne consegue che le soluzioni previamente esaminate, intervenendo proprio su questo aspetto, avranno al contempo un impatto positivo sul mercato.

[473] Reyna, Martin, Chen, Soler, Dìaz, (n. 439), 180.

Il fenomeno della "competizione sulla privacy" ha luogo infatti dal momento che le imprese dominanti sul mercato, abusando della propria posizione, possano eludere o addirittura violare l'applicazione della disciplina, sfruttando il vantaggio competitivo derivante dall'utilizzo dei dati personali, ulteriore rispetto a quanto possibile per le concorrenti che operano nell'osservanza della disciplina del GDPR. Se è la struttura stessa dei dispositivi a garantire il rispetto della normativa, tale possibilità viene meno. Sotto questo profilo, è proprio in virtù della convergenza e coincidenza delle due discipline che le soluzioni proposte avendo riguardo dell'una assumono validità anche qualora applicate all'altra. Dall'altro, tale impostazione si concilia con l'idea già discussa di favorire lo sviluppo di sistemi ispirati ai principi di *trasparency by design* o *security by design*. Intervenendo sul piano tecnico prima che normativo è infatti possibile studiare soluzioni che abbiano un impatto trasversalmente positivo e consentano la diffusione di sistemi in linea con tutte le disposizioni attualmente vigenti. Questo va a favore delle imprese più piccole, che dispongono di minori risorse e per le quali garantire il rispetto costante degli obblighi imposti dalle diverse discipline può divenire particolarmente oneroso. Una maggiore convergenza fra queste ultime, congiuntamente ad un intervento sul piano tecnico che consenta di adeguarsi più facilmente alle disposizioni vigenti, accrescerebbe la sostenibilità economica nel lungo termine, salvaguardando al contempo le imprese dal rischio di incorrere nell'irrogazione di sanzioni. Anche sotto questo profilo, può dunque dirsi che l'utilizzo congiunto di diverse tecnologie è una soluzione non soltanto percorribile, ma assolutamente auspicabile.

CONCLUSIONI

Il presente lavoro di tesi muove dalla volontà di dimostrare che, tenuto conto delle peculiarità dei nuovi mercati digitali, nonché dell'impatto decisivo che la diffusione delle nuove tecnologie ha sulle nostre vite, l'evoluzione normativa non può in alcun modo prescindere da una parallela evoluzione sul piano tecnologico. La sfida del futuro prossimo sarà quella di guardare a queste due realtà – legislativa e tecnica – congiuntamente, nella convinzione che l'una può giovare all'altra e viceversa.

In particolare, si è focalizzata l'attenzione sui sistemi *Internet of Things*, di cui si riconosce l'importanza a livello industriale e sociale. Si è voluto dimostrare che proprio attraverso l'integrazione di diverse tecnologie sarà possibile garantire la diffusione di una nuova generazione di sistemi compatibili con la disciplina vigente e i principi cardine dell'UE. Ci si è soffermati sui problemi relativi la tutela dei dati personali, ampliando l'analisi anche alla relazione fra questi ultimi e la concorrenza sul mercato. Partendo dall'innovativo principio affermato dal Bundeskartellamt, l'Autorità garante della Concorrenza tedesca, in una decisione contro Facebook[474] adottata nel 2019, secondo il quale la violazione della

[474] Si veda Capitolo I, para 1.3

disciplina sulla tutela dei dati può costituire al contempo un illecito concorrenziale, si è cercato di comprendere *lato sensu* quale sia la correlazione fra questi due settori e in che modo la loro convergenza possa influire sui futuri sviluppi.

Le soluzioni prospettate sono basate sulla convinzione che sfruttando la tecnologia *blockchain* e gli *smart contract*, il trattamento dei dati personali mediante sistemi IoT possa raggiungere più alti livelli di compatibilità con la disciplina UE, generando effetti positivi anche per la concorrenza.

Il fatto che la tecnologia non conosca confini geografici, ma la sua centralità sia ampiamente riconosciuta da tutti i Paesi, come dimostrato dai massicci investimenti nel settore fatti sia dagli USA che dalla Cina, determina un'urgenza d'intervento ancora maggiore[475]. Il rischio è che si diffondano standard comuni in contrasto rispetto ai princìpi cardine dell'UE.

L'analisi è stata condotta alla luce del quadro normativo attuale, analizzando in particolare la disciplina dettata dal Regolamento (UE) 2016/679 sulla protezione dei dati personali, che ha valorizzato il ruolo dell'UE nel panorama mondiale, attribuendole il ruolo di guida e di punto di riferimento nel settore. La *ratio* a cui si ispira il GDPR è quella di riconoscere ai soggetti interessati il pieno controllo dei propri dati personali, assumendo volutamente un atteggiamento neutro verso la tecnologia. Il concetto di neutralità tecnologica va inteso anzitutto nel senso che la disciplina dettata dal GDPR deve trovare applicazione a prescindere dal tipo di tecnologia impiegata mediante la quale viene eseguito il trattamento dei dati personali. Sotto un diverso profilo, la disciplina in esame può dirsi neutra nel senso che nell'adempiere agli obblighi che questa impone, il titolare del trattamento non è vincolato all'utilizzo di mezzi e/o strumenti specifici. Il legislatore europeo è stato lungimirante nel riconoscergli la libertà di disporre le misure più adeguate a garantire la piena tutela dei dati personali, senza limitare la possibilità di ricorrere all'utilizzo di nuove tecnologie a tale scopo.

Il quadro normativo europeo è divenuto un punto di riferimento anche per le altre giurisdizioni, che hanno finito con l'adattarsi agli standard da esso imposti. Ne sono un chiaro esempio i casi Schrems I e II[476], che hanno fatto emergere i rischi legati al trasferimento dei dati personali dall'UE verso gli USA, costringendo per ben due volte alla revisione della decisione di adeguatezza che lo disciplinava.

Dal punto di vista concorrenziale, però, la normativa vigente è carente ***nel senso di non riconoscere adeguatamente il valore economico dei dati.***

Questo ha impedito di valutare adeguatamente la posizione delle imprese sul mercato nel particolare contesto dei mercati multilaterali, caratterizzati da fenomeni quali gli effetti di rete, gli effetti *lock-in* e le economie di scala[477]. Inoltre, è stato sottovalutato il ruolo dei dati nella definizione dei modelli di

[475] Si veda Capitolo I, p. 57.
[476] Si veda nota 240.
[477] Si veda Capitolo I, para 1.2.

business adottati dalle imprese, che puntano alla personalizzazione delle offerte, dei beni e dei servizi sulla base delle preferenze manifestate dai consumatori. Grazie a tecniche di analisi algoritmica dei dati sempre più sofisticate, le imprese sono infatti in grado di carpire innumerevoli informazioni e sfruttare la profilazione dei consumatori. Maggiori sono le informazioni tratte dall'analisi dei dati, maggiore sarà il loro valore economico. La mole di informazioni varia sulla scorta di due elementi fondamentali: le tecniche di analisi utilizzate e la tipologia dei dati trattati. Quanto a quest'ultimo elemento, è evidente l'importanza assunta dai dati personali, che rivelano informazioni preziosissime da un punto di vista economico e commerciale.

Emerge così il legame esistente fra la disciplina concorrenziale e quella relativa alla tutela dei dati personali, tanto che si è giunti a parlare della cosiddetta "competizione sulla privacy"[478], alludendo con questa espressione al vantaggio competitivo legato all'applicazione della disciplina sulla tutela dei dati.

In questo contesto, la decisione del *Bundeskartellamt* contro Facebook potrebbe rivoluzionare il panorama europeo. Se la CGUE, a cui la questione è stata rimandata in via pregiudiziale, confermerà la legittimità dell'indirizzo ivi adottato, gli effetti sulla disciplina concorrenziale e soprattutto per le imprese, saranno notevolissimi. Per la prima volta si afferma che la violazione della disciplina sulla tutela dei dati personali possa costituire al contempo un illecito concorrenziale. Nel caso di specie, le *policy privacy* adottate da Facebook, con particolare riguardo dei dati personali di cui la piattaforma ha la disponibilità tramite terzi, sono state considerate come condizioni contrattuali abusive ai sensi dell'art. 102 TFUE. Se il principio venisse affermato a livello generale, le imprese correrebbero il rischio di incorrere in una duplice irrogazione di sanzioni.

A maggio 2021 la Commissione europea ha inoltre dichiarato l'intenzione di intraprendere una propria indagine contro Facebook, volta a verificare se il servizio di Marketplace offerto dalla piattaforma costituisca o meno un abuso di posizione dominante ai sensi dell'art. 102 TFUE. Gli utenti godono infatti della possibilità di scambiare gratuitamente prodotti e servizi, ma ciò – ed è quanto sostenuto dai concorrenti – determina una distorsione nel mercato della pubblicità[479].

Il panorama della disciplina UE sulla concorrenza è destinato a cambiare anche in conseguenza delle riforme che auspicabilmente saranno approvate nei prossimi mesi[480]. Fra le più rilevanti figurano le due proposte di Regolamento presentate dalla Commissione europea il 15 dicembre 2020 - il *Digital Market Act* e *Digital Service Act* – che hanno ad oggetto la regolamentazione dei mercati digitali e prevedono l'introduzione di diversi obblighi (soprattutto sulla condivisione dei dati) in capo ai cosiddetti

[478] Si veda capitolo I, pag. 27
[479] Espinoza, (n. 240).
[480] Si veda capitolo I, para 1.4.2.

"gatekeeper". Viene dunque riconosciuto sia il valore economico dei dati, che il legame fra la disciplina sulla concorrenza e quella relativa alla tutela dei dati personali.

Due elementi sono particolarmente degni di nota.

Il primo, che il Digital Market Act mutui dal GDPR il diritto alla portabilità dei dati, ampliandone la portata. La proposta della Commissione mira ad estendere la portata di questo diritto – nato già con una forte connotazione commerciale - sia sotto il profilo oggettivo che soggettivo. Il diritto alla portabilità potrà infatti essere esercitato anche con riferimento ai dati non personali da parte degli utenti *business*.

Quanto al secondo elemento, le proposte elaborate dalla Commissione mirano a favorire l'adozione di soluzioni *ex ante*, anziché interventi *ex post*, seguendo un approccio tipico della disciplina sulla tutela dei dati personali. La scelta della Commissione può spiegarsi alla luce del fatto che lo sfruttamento economico dei dati rappresenta senz'altro un rischio per la concorrenza nel mercato, ma ha al contempo delle implicazioni etiche e sociali di natura più ampia.

Le prospettive di riforma a livello europeo non sono però limitate alla sola regolamentazione dei mercati digitali, ad esempio, l'attuale Direttiva e-Privacy, che disciplina l'utilizzo dei dati personali nelle telecomunicazioni, dovrebbe assumere la forma di Regolamento, così da garantirne la diretta ed uniforme applicazione su tutto il territorio UE. Inoltre, il 21 aprile 2021 la Commissione ha presentato una proposta di Regolamento riguardante l'Intelligenza Artificiale[481]. Il provvedimento contiene, fra le altre, importanti disposizioni che dimostrano la grande attenzione del legislatore europeo verso la tutela dei dati personali. È prevista ad esempio la creazione delle cosiddette *"regulatory sandboxes"*, ossia degli spazi protetti di sviluppo dei nuovi sistemi, finalizzati a testare anticipatamente l'impatto di questi ultimi sui dati personali. L'indirizzo adottato dalla Commissione è quello di incoraggiare lo sviluppo delle nuove tecnologie, pur riconoscendo la necessità di intervenire già nella fase di progettazione e sviluppo.

Questo concetto è alla base del principio di *privacy-by-design* sancito dall'art. 25 del GDPR[482]. In virtù di tale disposizione, infatti, il titolare del trattamento è tenuto a favorire, già in fase di progettazione, l'adozione di soluzioni tecniche che garantiscano pienamente la tutela dei dati personali.

Basti pensare che la semplicità con cui, grazie all'utilizzo dell'AI e alla disponibilità di *datasets* diversi, le imprese sono in grado di giungere all'identificazione dell'individuo ha indotto la dottrina a sostenere che la disciplina sancita dal GDPR debba essere indistintamente applicata a tutti i dati trattati[483]. Il rischio insito nella dilatazione dell'ambito di applicazione della normativa è però quello di non garantirne la

[481] Commissione europea, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final.
[482] Si veda capitolo I, p. 56 e capitolo II p. 80
[483] Si veda capitolo I, p. 40 ss.

piena effettività. L'unica strada percorribile è favorire lo sviluppo di soluzioni innovative che ne assicurino il rispetto *by-design*. Ciò che è auspicabile è dunque la nascita di una nuova generazione di tecnologie strutturalmente compatibile con la normativa vigente. In questo modo sarebbe più facile anche favorire *de facto* la diffusione, la condivisione e il rispetto dei principi portanti della disciplina UE anche da parte degli altri Paesi.

Su queste considerazioni si basa la tesi qui sostenuta, cioè che grazie all'integrazione fra sistemi IoT, *blockchain* e *smart contract* sia possibile garantire una maggiore tutela dei dati personali, ottenendo al contempo effetti positivi sulla concorrenza[484].

Tutte le riflessioni previamente svolte sull'utilizzo dei dati e il loro sfruttamento economico e circa l'impatto di queste attività sugli individui e sulla tutela dei loro diritti fondamentali trovano infatti una propria dimensione pratica nel contesto specifico dei sistemi IoT, di cui sono esempi tipici le *"smart home"* e le *"smart city"*.

A dimostrazione della fondatezza di questa tesi, si è svolta un'analisi dettagliata volta a vagliare la compatibilità fra i sistemi IoT attualmente esistenti e la disciplina dettata dal GDPR, nonché di quella concorrenziale, mirando a metterne in luce gli aspetti più problematici.

Quanto al primo profilo, le criticità emerse variano a partire dalla difficoltà di definire con certezza l'ambito di applicazione del GDPR e garantire il rispetto dei principi previsti dall'art. 5 e dei diritti dell'interessato[485]. Si è posta particolare attenzione all'inadeguatezza delle basi giuridiche di cui all'art. 6 (in particolar modo del consenso), nonché sulla complessa ripartizione dei ruoli di responsabile e titolare del trattamento.

In merito invece al secondo profilo, riguardante il diritto alla concorrenza, si è affrontato il tema della proprietà dei dati e dei possibili comportamenti collusivi basati su algoritmi[486]. Quanto all'acquisizione di posizioni dominanti, è stata sottolineata la rilevanza delle barriere legali, costituite principalmente dai diritti di proprietà intellettuale e dalla disciplina sui dati personali. Per molti dei problemi ravvisati, a partire dalla poca trasparenza nelle modalità di trattamento dei dati, sino a giungere alla necessità di rafforzare i livelli di sicurezza del trattamento e garantire l'accuratezza dei dati raccolti, si è evidenziato che soluzioni promettenti deriverebbero proprio dallo sfruttamento della *blockchain* e degli *smart contract*.

[484] Si veda capitolo III
[485] Si veda capitolo II, para 2.1.2
[486] Si veda capitolo II, para 2.1.3

Nel prosieguo dell'analisi sono stati evidenziati i dubbi sulla compatibilità fra la *blockchain* e la disciplina del GDPR, illustrando come, anche in questo caso, la revisione della disciplina congiuntamente al progresso tecnologico possa consentirne un utilizzo sostenibile e sicuro.

E' emerso con chiarezza che occorre distinguere fra *blockchain* di tipo *permissioned* e *permissionless*, e che le prime garantiscono maggiore compatibilità rispetto alla disciplina sulla tutela dei dati[487]. Le incertezze maggiori sono legate all'assenza di un quadro normativo chiaro ed omogeneo, anche se è apprezzabile il tentativo di alcuni legislatori nazionali – fra cui quello italiano – di definire l'inquadramento giuridico di queste tecnologie.

Quanto agli *smart contract*, bisogna delineare chiaramente le condizioni necessarie perché questi siano effettivamente qualificabili come contratti e sarebbe auspicabile l'adozione di una disciplina uniforme a livello sovranazionale[488]. E' molto interessante constatare che anche il funzionamento di questi strumenti trarrebbe beneficio da una loro integrazione con i sistemi IoT. I singoli dispositivi che compongono i sistemi potrebbero infatti essere utilizzati in funzione di "oracoli", cioè come collegamento fra il mondo reale e gli *smart contract*[489]. Gli oracoli svolgono infatti l'importante ruolo di fornire i dati necessari per verificare se le condizioni necessarie all'attuazione del contratto si siano verificate o meno.

Occorre però fare un'altra importante premessa. Le soluzioni illustrate sono variegate e incidono su profili diversi. La scelta dell'una o dell'altra o il loro utilizzo congiunto dipenderà dunque dal contesto specifico nel quale tali sistemi dovranno essere utilizzati.

Esaminando i progetti già proposti, è possibile tracciare un quadro generale degli aspetti che trarrebbero maggior beneficio dall'integrazione fra sistemi IoT, *blockchain* e *smart contract*[490]. In primo luogo, la tecnologia *blockchain* potrebbe contribuire al miglioramento delle tecniche di anonimizzazione e pseudonimizzazione dei dati, in linea con quanto stabilito dal GDPR. Gli *smart contract* potrebbero inoltre rivelarsi uno strumento utilissimo per gestire i permessi di accesso ai dati, restituendo agli interessati il pieno controllo su di essi e garantendo loro una reale e piena informazione sui soggetti autorizzati al trattamento e sulle modalità con cui questo viene effettuato. La natura della *blockchain* favorirebbe il rispetto del principio di trasparenza, nonché di quello di sicurezza del trattamento, semplificando al tempo stesso l'adempimento degli obblighi da parte del titolare, in ossequio al principio di responsabilità sancito dall'ultimo comma dell'art. 5 del GDPR. La catena (*blockchain*) consente infatti di registrare tutte le operazioni eseguite sui dati, dando al titolare del trattamento la possibilità di dare una prova certa del proprio operato, dimostrando di avere correttamente adempiuto agli obblighi imposti dalla disciplina. L'immutabilità dei dati caricati e la natura decentralizzata della catena riducono inoltre

[487] Si veda capitolo II, para 2.2
[488] Si veda capitolo II, para 2.3.1
[489] Si veda capitolo II, p. 121
[490] Si veda capitolo III

i rischi legati a possibili attacchi informatici, garantendo maggiore sicurezza del trattamento. Infine, gli *smart contract* potrebbero consentire di traslare in codice le regole dettate dal GDPR e garantirne l'attuazione automatica e certa. Non si tratta di mere speculazioni o supposizioni, ma di soluzioni che sono già state messe in pratica – seppure nell'ambito di progetti pilota – proprio per migliorare la gestione delle *smart city*. Di particolare rilevanza in tal senso è il progetto DECODE, sviluppato nelle città di Barcellona ed Amsterdam e finanziato grazie ai fondi europei del programma Horizon2020[491].

Un profilo irrisolto è quello che riguarda l'individuazione del titolare e del responsabile del trattamento. Entrambe queste figure devono essere identificate seguendo un approccio di tipo funzionale, cioè guardando alle attività e soprattutto al controllo sul trattamento che ciascun soggetto è in concreto in grado di esercitare. Il discorso è stato largamente affrontato in dottrina sia riguardo ai sistemi IoT che alla *blockchain*, senza che si sia però giunti ad una soluzione univoca e certa[492]. Ciò che qui può suggerirsi è che la nascita di una nuova generazione di sistemi potrebbe contribuire a definire più chiaramente le funzioni svolte dai soggetti coinvolti nel trattamento, facilitando l'attribuzione dei singoli ruoli.

La correlazione fra la tutela dei dati personali e concorrenza sul mercato consente di giungere ad una conclusione ulteriore. Le soluzioni proposte operano – come si è più volte ribadito – sul piano tecnico. Il fenomeno della "competizione sulla privacy" troverebbe pertanto soluzione, dal momento che predisponendo dei sistemi che assicurano automaticamente il rispetto delle regole vigenti in materia di tutela dei dati, le imprese sarebbero private della possibilità di eludere la disciplina o di proporre delle condizioni diverse rispetto a quelle offerte dalle concorrenti. Verrebbe ristabilito l'equilibrio di mercato, arginando la possibilità che siano commessi abusi alla stregua di quanto accaduto nel caso Facebook contestato dal Bundeskartellamt.

Posto che gli effetti positivi sulla concorrenza derivanti dall'integrazione fra sistemi IoT, *blockchain* e *smart contract* sono qui analizzati con una prospettiva limitata agli aspetti che dipendono dal rapporto fra diritto alla concorrenza e tutela dei dati personali, può concludersi che vi siano almeno altri due elementi degni di nota.

In primo luogo, le soluzioni illustrate favoriscono l'interoperabilità dei sistemi, facilitando l'esercizio del diritto alla portabilità dei dati[493]. Utilizzando la stessa catena o *smart contract* che adottano il meccanismo di funzionamento, i vari sistemi, anche se creati da soggetti diversi, sarebbero in grado di comunicare fra loro. Le considerazioni previamente svolte sull'importanza rivestita dal diritto alla portabilità dei dati in ambito concorrenziale, sono sufficienti a far comprendere l'impatto che queste

[491] SI veda capitolo III, p. 131 ss.
[492] Si veda capitolo II, p. 88 e 112.
[493] Si veda capitolo III, p. 140 ss.

novità potrebbero avere nel futuro sviluppo dei sistemi. La creazione di standard comuni è centrale nella risoluzione di tutti i problemi legati all'acquisizione di posizioni dominanti sul mercato. E' quanto si è discusso ad esempio trattando delle barriere legali che possono influenzare l'equilibrio di mercato. Il corretto funzionamento dei sistemi IoT è infatti intrinsecamente legato all'adozione di standard comuni. Tale problema, al quale si è cercato di porre rimedio intervenendo esclusivamente sul piano normativo (cioè imponendo l'obbligo di condivisione degli standard) potrebbe essere risolto anteriormente, attraverso un intervento di tipo tecnico ispirato al rispetto dei principi e delle disposizioni dettate dalla legge.

Il secondo aspetto rilevante è di carattere più generale e riguarda la propensione dei recenti sviluppi della disciplina sulla concorrenza verso l'adozione di un approccio *ex ante* e il superamento della classica impostazione rimediale. Favorire un intervento di tipo preventivo, implica – fra le altre cose – l'applicazione del principio *by-design*. Il cambio di rotta della disciplina consente dunque di guardare con favore allo studio di soluzioni tecniche e preventive, volte alla creazione di sistemi e meccanismi che ne garantiscano il rispetto già a livello strutturale. A ciò si aggiunge una considerazione ulteriore. Se, come sembra, l'UE confermerà la validità della tesi sostenuta dal *Bundeskartellamt* contro Facebook, ammettendo definitivamente che violare la disciplina sulla tutela dei dati può costituire al tempo stesso un illecito concorrenziale, diviene ancora più rilevante garantire la compatibilità fra la prima e i futuri sistemi. Dal punto di vista delle imprese, infatti, questo nuovo indirizzo giurisprudenziale potrebbe rivelarsi particolarmente insidioso e rischioso, poichè a fronte di una singola condotta queste potrebbero incorrere nell'imposizione di più sanzioni. Si pone concretamente il rischio che, al fine di garantire una più ampia e certa tutela degli individui, venga posto un freno allo sviluppo dell'economia, in netto contrasto con la *ratio* che ispira l'intera disciplina dell'UE, ossia il rafforzamento del mercato interno unico. Il risultato di un intervento a monte è positivo sotto tutti i punti di vista: ne beneficiano gli utenti/utilizzatori finali, tutelati in quanto individui e consumatori, ma anche le imprese, al riparo dall'eventualità che vengano loro impartite pesanti sanzioni.

Un monito finale è però necessario. Promuovere lo sviluppo parallelo di tecnologia e legge, non può e non deve tradursi in un irragionevole favore per la prima a scapito della seconda. Sin dall'avvento di Internet e ai primissimi tentativi di regolamentazione che ne sono seguiti, si è subito compreso che le caratteristiche proprie della legge le impediscono di intervenire in modo effettivo ed efficace in contesti particolarmente innovativi e soggetti a continuo cambiamento. In primo luogo, questa si limita ad intervenire soltanto *ex post*, in circostanze in cui ciò non è sempre sufficiente a porre rimedio. La continua evoluzione della tecnologia fa sorgere inoltre il rischio che le norme introdotte divengano velocemente obsolete e inadeguate. Sebbene negli anni il legislatore abbia compreso la necessità di conferire alle norme un'apertura tale da consentirne l'adattamento a situazioni imprevedibili al momento della loro formulazione, in molti casi questo si è rivelato insufficiente a garantire una regolamentazione

efficace. L'effettività della legge è inoltre compromessa dalle difficoltà relative all'individuazione della giurisdizione competente e alla mancanza di un quadro normativo uniforme e condiviso fra i diversi Paesi. Giungere ad un tale risultato è comunque complesso, poiché le differenze fra i vari ordinamenti – specialmente confrontando quelli dei Paesi dell'UE ed extra-UE – sono notevoli e difficili da superare.

Il linguaggio matematico ha invece carattere universale e non dà luogo a problemi interpretativi, né di certezza nell'applicazione. Per tale ragione, col tempo si è fatta largo fra molti autori l'idea che le nuove tecnologie non potessero che essere regolamentate attraverso i loro stessi codici di programmazione. Il primo ad equiparare il codice (*code*) alla legge fu nel 1999 Lessig, il quale coniò l'emblematica espressione *"code is law"*[494]. In altre parole, partendo dal presupposto che ogni forma di regolamentazione esterna è insufficiente a garantire piena effettività, si afferma che questa possa essere ottenuta solo traducendo la disciplina in linguaggio computazionale e rendendola parte integrante della tecnologia. L'avvento della *blockchain*, spesso definita come una tecnologia "regolamentare", ha contribuito a riscoprire e rafforzare questa tesi[495]. Si sostiene infatti che attraverso il protocollo che regola il funzionamento della catena possa essere data attuazione alla disciplina voluta.

Con particolare riguardo al settore della privacy e della protezione dei dati, il concetto di *Legal Protection by Design* è stato ampiamente esplorato dalla dottrina, che ha ravvisato nell'inscindibile rapporto fra norma e tecnologia l'elemento fondamentale per garantire la piena attuazione dei principi legali e un'effettiva tutela degli individui[496]. Si tratta di riflessioni ampiamente condivise anche dall'ENISA, che ormai da tempo promuove le cosiddette *Privacy-Enhancing Technologies* (PETs)[497], termine con il quale si fa riferimento tecnologie architetturalmente idonee a garantire la tutela dei dati personali. Guardando al caso specifico dei sistemi IoT e alla loro possibile integrazione con *blockchain*, deve farsi riferimento ad un ulteriore parere rilasciato dall'ENISA, relativo all'impatto della *blockchain* sul rafforzamento dei livelli di sicurezza dei suddetti sistemi[498]. Posto che quest'ultimo è uno dei principi di cui il titolare del trattamento deve garantire il rispetto ai sensi del GDPR, s'intuisce la potenzialità di esplorare questo approccio.

Occorre qui chiarire due aspetti fondamentali. Anzitutto, bisogna tenere presente che i codici matematici sono caratterizzati da un estremo grado di precisione ed esattezza, mentre i concetti giuridici sono spesso e volutamente ampi e indefiniti, e l'individuazione del significato specifico ad essi attribuibile è subordinato ad un'interpretazione elaborata sulla base dei principi sanciti dall'ordinamento. La traslazione delle disposizioni normative in formule matematiche non è dunque agevole, né tantomeno

[494] Lawrence Lessig, "Code and other laws of cyberspace", (Basic Books, 1999).
[495] Si veda capitolo II, para 2.1.1
[496] Francesco Romeo, "Il governo giuridico delle tecniche dell'informazione e della comunicazione" in Vincenzo Cuffaro, Roberto D'Orazio, Vincenzo Ricciuto, e altri *I Dati Personali Nel Diritto Europeo,* 2019, (Torino, G. Giappichelli), 1273 ss.
[497] Sul punto si veda in generale ENISA, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies?tab=publications, ultimo accesso 30 maggio 2021.
[498] ENISA, "Guidelines For Securing The Internet Of Things, Secure supply chain for IoT", (n. 218).

immediata o sempre possibile. Il secondo aspetto ha invece a che fare con la legittimazione e la legittimità della legge. Slegare la regolamentazione delle nuove tecnologie dall'ordinamento giuridico vigente comporterebbe la creazione di un sistema parallelo ed autonomo rispetto a quest'ultimo. Se, in virtù della presunta superiorità del codice rispetto alla legge, si finisce con l'attribuire al primo assoluta indipendenza, ne consegue che, sebbene nella prassi la normativa trovi applicazione, questa sarebbe *de facto* esautorata. Il rischio, in altre parole, è quello di attribuire potere di regolamentazione ad un sistema che non gode della legittimazione necessaria per farlo ed a soggetti che non godono dell'investitura democratica da parte dei cittadini. Non si dimentichi, infatti, che i codici sono comunque frutto del lavoro di programmatori ed ingegneri, ai quali sarebbe così attribuito il ruolo che di regola spetta al legislatore. Svincolare la regolamentazione delle tecnologie dall'ordinamento giuridico farebbe venire meno la legittimità di intervento da parte delle autorità competenti e preposte ai controlli, privandole del potere di porre rimedio nel caso in cui siano ravvisabili errori e altre forme di illegittimità. L'attuazione automatica delle regole dettate dal codice non garantisce infatti l'intrinseca correttezza delle stesse. Se le regole sono elaborate inglobando errori pregressi, errate valutazioni o *bias* umani, queste continueranno a riproporsi nel tempo, a meno che non vi sia un intervento da parte di un soggetto esterno.

Tutte queste considerazioni portano ad una conclusione finale che vuole essere il messaggio ultimo di questo lavoro di tesi. Il progresso e l'evoluzione tecnologica hanno posto sfide nuove e di significativa importanza, mettendo a repentaglio addirittura il rispetto dei principi fondamentali. I tradizionali strumenti normativi di cui ci siamo serviti finora per porre rimedio a violazioni e abusi hanno mostrato nel corso del tempo i propri limiti. Non può più prescindersi dalla constatazione che la legge ha bisogno della tecnologia, almeno quanto la tecnologia ha bisogno della legge. L'una trae beneficio dal proficuo rapporto con l'altra e soltanto il loro sviluppo parallelo permetterà di trovare soluzioni adeguate alle esigenze che stanno emergendo. Non può guardarsi ad ognuna di esse come ad una realtà a sé stante, ma occorre tenere presente gli effetti positivi che possono scaturire dalla loro relazione. Lo stesso discorso può essere fatto – e ne sono un esempio IoT, *blockchain* e *smart contract* – riguardo alle singole tecnologie, ma anche in relazione ai diversi settori del diritto, come dimostra la convergenza fra diritto alla concorrenza e tutela dei dati personali. La realtà in cui viviamo chiede risposte all'altezza della propria complessità, che soltanto un approccio olistico e trasversale può permettere di trovare.

BIBLIOGRAFIA

Giurisprudenza

- Autorità Garante della Concorrenza e del Mercato *Big data, Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS* [2017], accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf (ultimo accesso 29 Aprile 2021).
- Autorità Garante della Concorrenza e del Mercato, *Facebook-Condivisione Dati Con Terzi* Provvedimento n. 27432 [2018], accessibile da http://www.agcm.it/dotcmsCustom/tc/2023/12/getDominoAttach?urlStr=192.168.14.10:8080/C12560D000291394/0/5A1EFA963A109B64C125835F00542FE2/%24File/p27432.pdf.
- Bundeskartellamt B6-22/16 *Facebook, exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* [2019].
- Bundeskartellamt, *Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing* [2019] case summary.
- C 6-72 *Europemballage Corpn and Continental Can Inc v Commission* (OJ)1972 L 7 25.
- C-457/10 *AstraZeneca AB and AstraZeneca plc v European Commission* [2012].
- C-32/11 *Allianz Ungheria* [2013] OJ C 141/3.
- C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González* [2014].
- C-141/12 *YS e altri c. Minister voor Immigratie, Integratie en Asiel* [2014].

- C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni*, [2015] OJ C-354/20.
- C-362/14 *Maximillian Schrems c. Data Protection Commissioner* [2015]
- C- 582/14 *Patrick Breyer c. Bundesrepublik Deutschland* [2016].
- C-434/16 *Peter Nowak c. Data Protection Commissioner* [2017].
- C-311/18 *Data Protection Commissioner c. Facebook Ireland and Maximillian Schrems* [2020].
- C-319/20 *Domanda di pronuncia pregiudiziale proposta dal Bundesgerichtshof (Germania) — Facebook Ireland Limited / Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V.* [2020] OJ C 359/2.
- Consiglio di Stato sezione VI, 29 marzo 2021, n. 2630.
- *Facebook/Whatsapp* (COMP/M 7217) Decision pursuant to Article 6(1)(b) of Council Regulation No 139/2004 C(2014) 7239 final OJ C 297.
- *Facebook/WhatsApp* (M. 8228) Decision imposing fines under Article 14(1) of Council Regulation (EC) No. 139/2004 for supply by an undertaking of incorrect or misleading information C(2017) 3192 final (2017) OJ C 286.
- Garante per la Protezione dei Dati Personali, Provvedimento n. 121 del 22 febbraio 2018 - Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento (UE) 2016/679.
- *Google/DoubleClick* (COMP/M.4621) Decision declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement C(2008) 927 final. (2008) OJ C 184.
- *EDF/Dalkia en France* (COMP. M.7137) Decisione della Commissione C(2014) 4438 final, (2014) OJ C 157.
- *Microsoft/LinkedIn* (M.8124) Decision pursuant to Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation No 139/2004 and Article 57 of the Agreement on the EEA, C(2016) 8404 final OJ C 388/4.
- Suprema Corte di Cassazione sezione I civile, n. 12381, 25/05/2021.

Legislazione

- Carta dei diritti fondamentali dell'Unione Europea, Parlamento Europeo, Consiglio e Commissione, (2000) C 202/389
- Decreto Legge. n. 135/2018.
- Direttiva del Parlamento Europeo e del Consiglio 2002/58/EC *del 12 Luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata del settore delle comunicazioni elettroniche* [2002] OJ L. 201/37.
- 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* [2019] OJ L. 172/56.
- Direttiva (UE) 2019/770 del Parlamento Europeo e Consiglio, *Direttiva relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali* [2019] OJ L. 136/1.
- Das Gesetz gegen Wettbewerbsbeschränkungen, Section 19(1).
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (GDPR) [2016] L 119/1.
- Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio *del 17 Aprile 2019 relativo all'ENISA, l'Agenzia l'Agenzia dell'Unione europea per la cybersicurezza, e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 2013/526* («regolamento sulla cybersicurezza»), [2019] OJ L 151.
- Risoluzione del Parlamento europeo 2020/2014, *Regime di responsabilità civile per l'intelligenza artificiale,* Risoluzione del Parlamento Europeo del 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale.
- Versione consolidata del Trattato sul Funzionamento dell'Unione Europea, (2008), OJ C 115/13.

Fonti secondarie

- -- "Big tech faces competition and privacy concerns in Brussels", The Economist, (2019), https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels.

- -- “DECODE”, https://decodeproject.eu/what-decode.
- -- “EU needs new teeth as watchdog of Big Tech”, *Financial Times*, (USA, 16 dicembre 2020), https://www.ft.com/content/6d4b9dbc-c795-427d-b43e-741a26511abb.
- -- “Europe’s beef with GAFA – big tech faces competition and privacy concerns in Brussels”, *The Economist* (2019), https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels.
- -- “Legal ontology to support contracts in DECODE scenarios”, DECODE project (2020), https://decodeproject.eu/publications/decode-legal-ontology-smart-contracts.
- -- “Privacy strategies for de DECODE architecture", DECODE project, (2019), https://decodeproject.eu/publications/privacy-design-strategies-decode-architecture-0.
- -- “Smart contracts for data commons”, DECODE project, (2019), https://decodeproject.eu/publications/smart-contracts-data-commons.
- Ali M. S, Vecchio M, Pincheira M e altri, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey”, 2019, vol. 21 no. 2 *IEEE Communications Surveys and Tutorials*, accessibile da https://s3-us-west-2.amazonaws.com/ieeeshutpages/xplore/xplore-ie-notice.html.
- Article 29 Working Party, Opinion 05/2014, “Opinion on anonymization techniques”, (2014).
- --, “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679”.
- --, “Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679”.
- Autorità Garante della Concorrenza e del Mercati, Autorità Garante delle Comunicazioni, Autorità Garante per la protezione dei dati personali, *Indagine conoscitiva sui Big Data*, (2017), accessibile da https://www.agcm.it/dotcmsdoc/allegati-news/IC_Big%20data_imp.pdf.
- Autoritè de la concurrence e Bundeskartellamt, *Report ‘Competition law and data’*, (2016), accessibile da https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf;jsessionid=683860639BF2C0191A70260BE8486FDC.1_cid371?__blob=publicationFile&v=2.
- Barati M, Petri I, Rana O, “Developing GDPR Compliant User Data Policies for Internet of Things”, (2019). Proceedings of the 12th IEEE/ACM International Conference on Utility and Cloud Computing, https://doi.org/10.1145/3344341.3368812.
- Battelli E, D’Ippolito G, “Il diritto alla portabilità dei dati” in Tosi, Emilio, Antonello Soro, Vincenzo Franceschelli, Giovanni Buttarelli e Ettore Battelli *Privacy Digitale: Riservatezza e Protezione Dei Dati Personali Tra GDPR e Nuovo Codice Privacy*, 2019, (Vol. 21. Milano: Giuffrè Francis Lefebvre,).
- Benvenuto C, Mascolo P M, “Data Governance Act, verso uno spazio comune europeo dei dati: scenari e conseguenze”, (2020), *Agenda Digitale*, https://www.agendadigitale.eu/.
- Borgia E, “The Internet of Things Vision: Key Features, Applications and Open Issues”, (2014), vol. 54 *Computer Communications*, https://www.sciencedirect.com/science/article/pii/S0140366414003168?via%3Dihub.
- Bundeskartellamt, *Background information on the Facebook proceeding*, (2018), accessibile da https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Diskussions_Hintergrundpapiere/2017/Hintergrundpapier_Facebook.pdf;jsessionid=23A62F7CF5798330201105AA27D28631.1_cid362?__blob=publicationFile&v=6.
- Butterworth M, "The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, https://www.sciencedirect.com/science/article/pii/S026736491830044X?via%3Dihub.
- Carli S, “Gaia X, così l’Europa inizia a dettare legge sulla Nuvola”, *La Repubblica*, (30 Novembre 2020)
- Cavoukian A Ph.D, Information & Privacy Commissioner, Ontario, Canada, “Privacy by design - The 7 Foundational principles. Implementation and mapping of fair information practises”, (2010), accessibile da https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.
- Chee F Y, “Exclusive: EU’s Vestager warns Apple to treat all apps equally amid privacy dispute”, *Reuters* (8 Febbraio 2021), https://www.reuters.com/article/idUSL1N2KE243.
- Commissione Europea, *Comunicazione della Commissione, Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti* (2009) C45/7, para 10.

- Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio, La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati,* COM(2020) 264 final.
- Commissione Europea, *Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale* (Comunicazione) C 11/2.
- Commissione Europea, *Proposta per una Direttiva del Parlamento europeo e del Consiglio su certi aspetti concernenti i contratti per la fornitura di servizi digitali,* COM (2015).
- Commissione Europea, *Proposta di Regolamento del Parlamento Europeo d Del Consiglio del 10 gennaio 2017 relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE [2017]* COM/2017/010 final.
- Commissione Europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE* COM(2020) 725.
- Commissione Europea, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)* COM(2020) 842 final.
- Contaldo F, Campara F, Limone D A, e altri, "Blockchain, Criptovalute, Smart Contract, Industria 4.0: Registri Digitali, Accordi Giuridici e Nuove Tecnologie", 2019, (Pisa, Pacini giuridica).
- Costa-Cabral F, Lynskey O, "Family Ties: The Intersection between Data Protection and Competition in EU Law", (2017), vol. 54 no. 1 *Common Market Law Review*, http://eprints.lse.ac.uk/id/eprint/68470.
- De Caria R, "Definitions of smart contracts – between law and code", in Di Matteo, Larry A, Michel Cannarsa, e Cristina Poncibò *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, 2020, (Cambridge: Cambridge University Press), accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.
- De Filippi P, Wright A, "The future of organization" in *Blockchain and the Law: The Rule of Code*, 2018, (Cambridge: Harvard University Press), accessibile da https://www.jstor.org/stable/j.ctv2867sp.
- De Hert P, Papakonstantinou V, Malgieri G, Beslay L, Ca I, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, https://www.sciencedirect.com/science/article/pii/S0267364917303333?via%3Dihub.
- Dehghantanha A, Raymond Choo K, *Handbook of Big Data and IoT Security,* 2019, (ed. Cham: Springer International Publishing), accessibile da https://link.springer.com/book/10.1007%2F978-3-030-10543-3.
- ENISA, "Guidelines For Securing The Internet Of Things, Secure supply chain for IoT", (2020).
- Esayas S Y, "Competition in (Data) Privacy: 'zero'- Price Markets, Market Power, and the Role of Competition Law", (2018), vol. 8 no. 3 *International Data Privacy Law*, https://academic.oup.com/idpl/article/8/3/181/5198968.
- Espinoza J, "Brussels to open formal antitrust probe into Facebook", *The Financial Times*, (2021), accessibile da https://www.ft.com/content/3750ad46-04c3-4010-9fc1-fe2427c8520c.
- European Commission, *"Communication from the Commission to the European Parliament, the Council and the European Economic And Social Committee Setting out the EU approach to Standard Essential Patents" (Communication),* COM(2017) 712 final.
- European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and social Committee and the Committee of the Regions, A European Data Strategy*, COM(2020) 66 final.
- European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, COM (2020) 767 final 2020/0340 (COD).
- European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts* COM(2021) 206 final.
- European Data Protection Board, "Guidelines 05/2020 on consent under Regulation (UE) 2016/679", accessibile da https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
- European Data Protection Supervisor, Preliminary Opinion, "Privacy and competitiveness in the age of big data", (2014), accessibile da https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

- European Data Protection Supervisor, Opinion 8/2016, "Opinion on coherent enforcement of fundamental rights in the age of big data", (2016), accessibile da https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.
- European Parliament Think Thank, "Is Data Protection the new oil? Competition Issues in the digital economy", (2020), accessibile da https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2020)646117.
- European Parliamentary Research Service, "Blockchain and the General Data Protection Regulation - Can distributed ledgers be squared with European data protection law?", (2019), accessibile da https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.
- European Union Agency for Fundamental Rights, European Court of Human Rights, Council of Europe, "Handbook on European data protection handbook", (2018).
- Ezrachi A, Stucke E M., "Artificial intelligence & collusion: when computers inhibit competition", (2017), vol. 2 no. 5 *University of Illinois Law Review*, https://heinonline.org/HOL/P?h=hein.journals/unilllr2017&i=1816.
- Fabiano N, "Blockchain and Data Protection: The Value of Personal Data", (2018) vol. 16 no. 6 *Journal of Systemics, Cybernetics and Informatics*, http://www.iiisci.org/Journal/CV$/sci/pdfs/ZA165NO18.pdf.
- --, "GDPR & privacy: consapevolezza e opportunità. Analisi ragionata della protezione dei dati personali fra etica e cybersecurity", 2019, (Go Ware) https://www.perlego.com/book/1078890/gdpr-privacy-consapevolezza-e-opportunit-analisi-ragionata-della-protezione-dei-dati-personali-tra-etica-e-cybersecurity-prefazione-di-giovanni-buttarelli-pdf.
- Finck M, "Blockchain Regulation and Governance in Europe", 2019, (Cambridge: Cambridge University Press), accessibile da https://www.cambridge.org/core/books/blockchain-regulation-and-governance-in-europe/A722E0522BC6C5300AA0813340BD6C04.
- --, "Smart Contracts as a Form of Solely Automated Processing Under the GDPR", (2019), vol. 9 no. 2 *International Data Privacy Law*, accessibile da https://academic.oup.com/idpl/article/9/2/78/5488488.
- Foroohar R, "The FTC strikes back against Facebook", *The Financial Times*, 14 dicembre 2020.
- Gambino A M, Manzi M, "L'intelligenza artificiale tra protezione del consumatore e tutela della concorrenza", in Ruffolo, Ugo, Guido Alpa, Augusto Barbera, A. Barbera, G. Alpa, and U. Ruffolo *Intelligenza Artificiale: Il Diritto, i Diritti, l'Etica*, 2020, (Milano: Giuffrè Francis Lefebvre).
- Gatteschi V, Lamberti F, Demartini C, "Technology of smart contracts", in Di Matteo, Larry A., Michel Cannarsa e Cristina Poncibò *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, 2020, (Cambridge: Cambridge University Press), accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.
- Goldwasser S, Micali S, Rackoff C, "The knowledge complexity of interactive proof systems", 1989, Vol 18, No. 1 *Society for Industrial and Applied Mathematics*, accessibile da https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Proof%20Systems/The_Knowledge_Complexity_Of_Interactive_Proof_Systems.pdf.
- Gruppo di esperti del MISE sull'Intelligenza Artificiale, "Proposte per una strategia italiana sull'Intelligenza Artificiale", (2020), accessibile da https://www.mise.gov.it/index.php/it/198-notizie-stampa/2041246-intelligenza-artificiale-online-la-strategia.
- Hacker P, "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things", (2017), vol. 7 no. 4 *International Data Privacy Law*, https://academic.oup.com/idpl/article/7/4/266/4102081.
- Hassan M U, Rehmani M H e Chen J, "Privacy Preservation in Blockchain Based IoT Systems: Integration Issues, Prospects, Challenges, and Future Research Directions", (2019), vol. 97 *Future Generation Computer Systems*, accessibile da https://www.sciencedirect.com/science/article/pii/S0167739X18326542?via%3Dihub.
- Haucap J, "Competition and Competition Policy in a Data-Driven Economy", (2019), vol. 54/no. 4 *Inter Economics*, accessibile da https://link.springer.com/article/10.1007/s10272-019-0825-0.
- High-level expert group on Artificial Intelligence set up by European Commission, "Ethics guidelines for trustworthy AI", (2019).
- Information Commissioner's Officer, "Big Data, artificial intelligence, machine learning and data protection", (2018), accessibile da https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

- Jabed M, Chowdhury M, Ferdous M S, Biswas K, e altri "A Survey on Blockchain-Based Platforms for IoT use-Cases", (2020), vol. 35 *Knowledge Engineering Review*, https://www.cambridge.org/core/journals/knowledge-engineering-review/article/survey-on-blockchainbased-platforms-for-iot-usecases/0E0A4C27EEBAA12139E6C80D49C03BF2.
- Joint Research Center (Commission), "The EU Digital Markets Act - A Report from a Panel of Economic Experts", (2021), accessibile da https://publications.jrc.ec.europa.eu/repository/handle/JRC122910.
- Khan L, "Amazon's Antitrust Paradox", (2017), vol. 126 no. 3 *The Yale Law Journal*, https://www.yalelawjournal.org/note/amazons-antitrust-paradox.
- Kosba A, Miller A, Shi E, e altri "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts", (2016), Proceedings - 2016 IEEE Symposium on Security and Privacy, accessibile da https://s3-us-west-2.amazonaws.com/ieeeshutpages/xplore/xplore-ie-notice.html..
- Kraus D, Obrist T, Hari O, e altri, "Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law", 2019, (Northampton, Ma, USA; Cheltenham, UK; Edward Elgar).
- Lachlan U, Neelima S, McAuley D, "Realising the Right to Data Portability for the Domestic Internet of Things", (2018), vol. 22 no. 2 *Personal and Ubiquitous Computing*, accessibile da https://link.springer.com/article/10.1007/s00779-017-1069-2.
- Lessig L, "Code and other laws of cyberspace", 1999, (Basic Books).
- Liguori L, Masarà E, "Quel braccio di ferro fra privacy e concorrenza dietro il caso Apple", *Wired*, (17 marzo 2021), https://www.wired.it/economia/business/2021/03/17/apple-privacy-concorrenza-antitrust/.
- Llanos J T, "A Close Look on Privacy Protection as a Non-Price Parameter of Competition", (2019), vol. 15/no. 2-3 *European Competition Journal*, accessibile da https://www.tandfonline.com/doi/full/10.1080/17441056.2019.1644577.
- Lokke M, "Blockchain and Data Protection" in Di Matteo, Larry A., Michel Cannarsa, e Cristina Poncibò *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, 2020, (Cambridge: Cambridge University Press), accessibile da https://www.cambridge.org/core/books/cambridge-handbook-of-smart-contracts-blockchain-technology-and-digital-platforms/BCDDFAAD7B661E6C268941ACA76B3A58.
- Lundqvist B, "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet-of-Things World: The Issue of Accessing Data", 2018, (Berlin, Heidelberg, Springer Berlin Heidelberg), https://doi.org/10.1007/978-3-662-57646-5_8.
- Madaan N, Ahad M A, Sastry S M, "Data Integration in IoT Ecosystem: Information Linkage as a Privacy Threat", (2018), vol. 34 no. 1, *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917301358?via%3Dihub.
- Maggiolino M, "L'intelligenza artificiale e l'accesso ai dati: un ruolo per il codice del consumo e per il diritto antitrust" in Ruffolo, Ugo, Guido Alpa, Augusto Barbera, A. Barbera, G. Alpa, e U. Ruffolo *Intelligenza Artificiale: Il Diritto, i Diritti, l'Etica*, 2020, (Milano: Giuffrè Francis Lefebvre).
- Maggiolino M, Colangelo G, "Data Protection in Attention Markets: Protecting Privacy through Competition?", (2017), vol. 8 no. 6 *Journal of European Competition Law & Practice*, accessibile da https://academic.oup.com/jeclap/article/8/6/363/3812670.
- Malgieri G, Custers B, "Pricing Privacy – the Right to Know the Value of Your Personal Data", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917302819?via%3Dihub.
- Mantelero A, "Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection", (2016), vol. 32 no. 2 *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364916300280?via%3Dihub.
- Mantelero A, Vaciago G, "Internet of things (IoT)" in Panetta, Antonio, Augusta Iannini, Guido Alpa, Stefano Rodotà, S. Rodotà, e G. Alpa *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)*, 2019, (Milano: Giuffrè Francis Lefebvre).
- Mayer-Schonberger V, Cate F H, "Notice and Consent in a World of Big Data", (2013), vol. 3 no. 2, *International Data Privacy Law*, accessibile da https://academic.oup.com/idpl/article/3/2/67/709124..
- Mayer-Schönberger V, Padova Y, "Regime Change? Enabling Big Data through Europe's New Data Protection Regulation", (2016), *Science and Technology Law Review*, https://doi.org/10.7916/stlr.v17i2.4007.

- Martinelli S, "Diritto all'Oblio e Motori Di Ricerca: Memoria e Privacy Nell'Era Digitale", 2017, (Vol. 5 no. 5, Milano: Giuffrè,).
- Mik E, "Smart Contracts: Terminology, Technical Limitations and Real World Complexity", (2017), vol. 9 no. 2 *Law, Innovation and Technology*, accessibile da https://www.tandfonline.com/doi/full/10.1080/17579961.2017.1378468.
- Minuto Rizzo A, "I profili antitrust del nuovo web e della nuova economia digitale", (2019), vol. 2 *Il Diritto Industriale*.
- Naudts L, "How machine learning generates unfair inequalities and how data protection instruments may help in mitigating them", in Leenes, Ronald, Rosamunde van Brakel, Serge Gutwirth, e Paul de Hert *Data Protection and Privacy: The Internet of Bodies*, 2018, (London: Bloomsbury Publishing Plc), https://www.perlego.com/book/875482/data-protection-and-privacy-the-internet-of-bodies-pdf.
- Prof. Dr. Mitrou L, "Is the general data protection Regulation (GDPR) 'artificial-intelligence proof?", (2018), https://ssrn.com/abstract=3386914.
- Moritz H, "Artificial Intelligence and Competition Law" in Wischmeyer Thomas e Timo Rademacher *Regulating Artificial Intelligence*, 2020, (1st ed. Cham: Springer International Publishing), accessibile da https://link.springer.com/chapter/10.1007%2F978-3-030-32361-5_16.
- Nuttall C, "UK tech rules may single out Facebook, Google", *Financial Times*, (8 dicembre 2020), https://www.ft.com/content/4a66cb73-8c30-4117-a4f7-d5de18f0e66b.
- Organization for Economic Co-operation Development (OECD), *Guidelines governing the protection of privacy and transborder flows of personal data, Annex to the Recommendation of the Council of 23th September 1980*, (1980).
- Palmieri A, Pardolesi R, "Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google", 2014, Quaderno n. 1 *Nuovi Quaderni del Foro Italiano*.
- Panarello A, Tapas N, Merlino G, Longo F, Puliafito A, "Blockchain and Iot Integration: A Systematic Survey", (2018), vol.18 no. 8 *Sensors* (Basel, Switzerland), accessibile da https://www.mdpi.com/1424-8220/18/8/2575.
- Pappagallo U, Durante M, Monteleone S, "What is new with the Internet of things in privacy and data protection? Four legal challenges on sharing and control in IoT" in Hert, Paul De, Serge Gutwirth, Rosamunde van Brakel e Ronald Leenes *Data Protection and Privacy: (in)Visibilities and Infrastructures*, 2017, (Springer International Publishing).
- Podszun R, "Standard Essential Patents and Antitrust Law in the Age of Standardisation and the Internet of Things: Shifting Paradigms", (2019), vol. 50, no. 6 *IIC - International Review of Intellectual Property and Competition Law*.
- Pollicino O, "Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain", (2014), fascicoli 4-5 *Il diritto dell'informazione e dell'informatica*.
- Purtova N, "The Law of Everything: Broad Concept of Personal Data and Future of EU Data Protection Law", (2018), vol. 10 no. 1, *Law, Innovation and Technology*, https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176.
- Raskin M, "The Law and Legality of Smart Contracts", (2017), vol. 304 *Georgetown Law Technology Review*, accessibile da https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2842258.
- Reyna A, Martín C, Chen J, Soler E, Díaz, "On Blockchain and its Integration with IoT. Challenges and Opportunities", (2018), vol. 88 *Future Generation Computer Systems*, accessibile da https://www.sciencedirect.com/science/article/pii/S0167739X17329205?via%3Dihub.
- Ricciuto V, "I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato", in Nadia Zorzi Galgano vol. 175 *Persona e Mercato Dei Dati: Riflessioni Sul GDPR*, 2019, (Milano, Padova, Wolters Kluwer).
- Robertson V H S E, "Excessive Data Collection: Privacy Considerations and Abuse of Dominance in the Era of Big Data", (2020), vol. 57, no. 1 *Common Market Law Review*, https://tinyurl.com/yfzqpls7.
- Romeo F, "Il governo giuridico delle tecniche dell'informazione e della comunicazione" in Vincenzo Cuffaro, Roberto D'Orazio, Vincenzo Ricciuto, e altri *I Dati Personali Nel Diritto Europeo*, 2019, (Torino, G. Giappichelli)

- Rose K, Eldridge S, Chapin L, "The Internet of Things: an overview. Understanding the issues and challenges of a more connected world", (2015), *The Internet Society*, https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf.
- Sammarco P, "Privacy digitale, motori di ricerca e social network: dal diritto di accesso e rettifica al diritto all'oblio condizionato" in Tosi Emilio, Antonello Soro, Vincenzo Franceschelli, Giovanni Buttarelli, and Ettore Battelli *Privacy Digitale: Riservatezza e Protezione Dei Dati Personali Tra GDPR e Nuovo Codice Privacy*, 2019 (Vol. 21. Milano: Giuffrè Francis Lefebvre).
- Sandbu M, "Regulation alone will not strengthen Europe's digital sector", *Financial Times*, (USA, 21 dicembre 2020), https://www.ft.com/content/53458590-4a33-4f11-9e1d-6d9c0b8ea5c1.
- Schneider G, "Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's Investigation Against Facebook", (2018), vol. 9 no. 4 *Journal of European Competition Law & Practice*, accessibile da https://academic.oup.com/jeclap/article/9/4/213/4903311.
- Sidharth C, "Artificial Intelligence - a Competition Law Perspective", (2019), vol. 40, no. 3 *European Competition Law Review*, https://tinyurl.com/yf9qn2s5.
- Stojanovic M, "Can Competition Law Protect Consumers in Cases of a Dominant Company Breach of Data Protection Rules?", (2020), vol. 16 no. 2-3 *European Competition Journal*, accessibile da https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1824464.
- Stuart L, Lipton A B, "An Introduction to smart contracts and their potential and inherent limitations", 2018, (Harvard Law School Forum on Corporate Law), accessibile da https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.
- Szabo N, "Smart Contracts", (1994).
- Tommaso M, "I Big Data tra protezione dei dati personali e diritto alla concorrenza" 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): Scritti in Memoria di Stefano Rodotà*, 2019, (Milano: Giuffrè Francis Lefebvre).
- Treccani, "Dizionario di Economia e Finanza", (2012), accessibile da https://www.treccani.it/enciclopedia/lock-in_%28Dizionario-di-Economia-e-Finanza%29/#:~:text=lock%20in%20Fenomeno%20che%20si,disponibili%20alternative%20potenzialmente%20pi%C3%B9%20efficienti-
- --, "Neologismi", (2019), accessibile da https://www.treccani.it/vocabolario/deep-learning_(Neologismi).
- Turner S, Quintero J G, Turner S, Lis J, Tanczer L M, "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment", (2020), *New Media & Society*, accessibile da https://journals.sagepub.com/doi/10.1177/1461444820934033.
- Wachter S, "Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR", (2018), vol. 34, no. 3 *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364917303904?via%3Dihub.
- --, "The GDPR and the Internet of Things: A Three-Step Transparency Model", (2018), vol. 10 no. 2 *Law, Innovation and Technology*, accessibile da https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1527479-
- Whish R, Bailey D, "Competition Law", 2018, (Oxford University Press).
- Václav J, "Ownership of Personal Data in the Internet of Things", (2018), vol. 34, no. 5 *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S0267364918300487?via%3Dihub.
- Van der Wees A, Breeuwsma J, Van Sleen A, "IoT Societal Impact – Legal Considerations and Perspectives" in Dr. Ovidiu Vermesan, Dr. Peter Friess *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*, 2016, *River Publishers*, https://digital-strategy.ec.europa.eu/en/library/digitising-industry-internet-things-connecting-physical-digital-and-virtual-worlds.
- Veale M, Edwards L, "Clarity, Surprises, and further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", (2018), vol. 34 no. 2 *The Computer Law and Security Report*, accessibile da https://www.sciencedirect.com/science/article/pii/S026736491730376X?via%3Dihub.
- Visconti Moro R, "Danno antitrust e piattaforme digitali", (2021), vol. 1 *Il Diritto industriale*.