La rivoluzione digitale ha trasformato la struttura dei mercati delle comunicazioni elettroniche, ridisegnando l'impatto di dati, reti e tecnologie sul sistema economico, politico e umano. Questo *Volume* offre una lettura sistemica di questi mutamenti, invitandoci a riflettere sull'evoluzione normativa posta dalle sfide della tecnica, che ha dilatato il suo ambito soggettivo dagli operatori di telecomunicazioni a nuovi attori, gli *Over The Top* (OTT), rivendicando una domanda di uguaglianza nelle regole.
In questo contesto, i contributi qui raccolti esaminano lo slittamento del baricentro regolatorio europeo alla luce dell'incidenza sui diritti fondamentali delle tecnologie emergenti (dai *Big data* alle neurotecnologie, fino all'Intelligenza artificiale). Queste ultime hanno messo in tensione le tradizionali categorie giuridiche e rivelato la fragilità dell'impianto *e-Privacy*, l'inconsistenza dell'asimmetria regolatoria fra Telco e OTT, e l'inadeguatezza dell'attuale *governance* dei dati rispetto alla complessità del presente.
Il Volume offre metodo e chiavi interpretative per orientarsi in questa transizione incerta, dove il diritto è costretto a misurarsi con una tecnica che cambia più rapidamente delle sue stesse definizioni. Sullo sfondo una domanda decisiva: quale architettura regolatoria sarà in grado di tenere insieme sicurezza, concorrenza e sviluppo tecnologico in linea con il progetto europeo?
La riflessione, che attraversa i contributi, muove da un principio comune: immaginare un diritto "constitutional by design", in cui Tecnica e Politica tornino a parlarsi, riconoscendo che solo in questa cooperazione si potrà costruire un ecosistema digitale capace di tutelare i diritti e, allo stesso tempo, di accogliere l'innovazione.

Giovanna De Minico è professoressa ordinaria di Diritto costituzionale e pubblico presso l'Università degli Studi di Napoli Federico II. Ha scelto temi di ricerca apparentemente distanti – Autorità indipendenti; regolazione alternativa all'eteronomia; terrorismo e Costituzione; diritti fondamentali e Internet; Intelligenza artificiale e assetto dei poteri; riforme costituzionali in corso – che si incontrano sul terreno delle nuove sedi della decisione politica. Su questi oggetti ha scritto libri, curatele e articoli scientifici. Componente del *Board* sull'Intelligenza artificiale dell'Autorità per le Garanzie nelle Comunicazioni. Co-coordinatrice del gruppo di ricerca internazionale *Constitutions in the age of Internet* dell'*International Association of Constitutional Law*. Osservatrice permanente dell'Accademia dei Lincei. *Legal Chief* dei Partenariati FAIR e RESTART, co-finanziati PNRR-MIUR. Editorialista del *Sole 24 Ore*, in rubrica *Commenti*.

Marco Orofino è professore ordinario di Diritto costituzionale e pubblico presso l'Università degli Studi di Milano dove insegna Diritto costituzionale, Informazione e Costituzione e Diritto dei dati e società digitale. La sua attività scientifica ha ad oggetto la regolazione delle reti e dei servizi di comunicazione elettronica, la *governance* dei dati e l'impatto delle trasformazioni digitali e del processo di integrazione europea sui diritti fondamentali, con particolare attenzione alla libertà di espressione, al diritto alla riservatezza e alla protezione dei dati personali e al diritto alla salute. È stato recentemente autore di libri e saggi dedicati alla disciplina europea dell'intelligenza artificiale e del cd. *Digital Package*. Partecipa a progetti di ricerca nazionali e internazionali sui temi della regolazione delle comunicazioni elettroniche, della protezione dei dati personali e del diritto all'oblio.

ISBN
9 788824 329934

€ 36,00

REGOLE TELECOMUNICAZIONI DATI NELL'EUROPA DIGITALE

# Regole telecomunicazioni dati nell'Europa digitale

a cura di

Giovanna De Minico e Marco Orofino

JOVENE

Regole telecomunicazioni dati
nell'Europa digitale

# Regole telecomunicazioni dati nell'Europa digitale

a cura di

Giovanna De Minico e Marco Orofino

JOVENE

Volume pubblicato con il contributo dell'Università degli Studi di Milano nell'ambito del Progetto PNRR REFERENCES - *REgulatory Frameworks, Equity/neutRality, experimEntal facilities, and user perceptioN of teChnology in Emerging networks and Services* - Bando a cascata RESTART - «*RESearch and innovation on future Telecommunications systems and networks, to make Italy more smART*».

Si ringrazia la Dott.ssa Lavinia Del Corona per la preziosa e puntuale attività di coordinamento.

In copertina: immagine progettata da Freepik, elaborazione grafica di Jovene editore.



ISBN 9788824329897

JOVENE EDITORE
Via Mezzocannone 109 - 80134 NAPOLI
Tel. (+39) 081 552 10 19 / 12 74 / 34 71
www.jovene.it info@jovene.it



Stampato in Italia *Printed in Italy*

# INDICE

# PREFAZIONE

Il presente volume raccoglie i risultati scientifici del progetto *Net4Future* e della *cascade call References*, un percorso che ha favorito la collaborazione fra università, ricercatori e istituzioni sui temi cruciali della regolazione digitale, delle telecomunicazioni e della tutela dei diritti fondamentali nell'ecosistema tecnologico contemporaneo.

*Net4Future* ha perseguito l'obiettivo di mettere in relazione competenze giuridiche, tecnologiche ed economiche in un contesto caratterizzato da rapidità dei mutamenti, crescente complessità regolatoria e progressiva interdipendenza tra infrastrutture digitali, dati e mercati. La *cascade call References* ha arricchito questo disegno, coinvolgendo studiosi, che, nei contributi qui esposti, percorrono con approcci complementari le molteplici dimensioni della trasformazione digitale con particolare attenzione al tema della regolazione dei dati.

I saggi di questo volume testimoniamo la ricchezza delle riflessioni elaborate da studiose e studiosi, un gruppo che, partendo da idee individuali, ha provato a incontrarsi su un terremo comune.

I contributi dei curatori, Giovanna De Minico e Marco Orofino, con cui l'opera si apre, affrontano i fondamenti della regolazione delle comunicazioni elettroniche, ricostruendo la genealogia del settore e le tensioni aperte dall'evoluzione normativa.

In questo scenario, il saggio di Giovanna De Minico offre una riflessione ampia sulla relazione che tiene insieme regole, tecnica e telecomunicazioni, cogliendo la stretta interdipendenza tra architetture regolatorie, poteri pubblici, mercati e diritti fondamentali. La sua analisi mostra come la storia passata e presente delle comunicazioni elettroniche sia stata segnata da un costante tentativo di comporre una misura di coesistenza tra innovazione e *Lex mercatoria*,

ma anche tra preoccupazioni securitarie e garanzia dei diritti fondamentali. L'Autrice tratteggia un inedito scenario per l'ecosistema digitale, che corre su coordinate sovranazionali, dove la tecnica diventa l'immancabile opportunità del nuovo millennio, purché usata a beneficio di tutti, imprenditori e cittadini. Diversamente, cioè se dovesse favorire solo una ristretta cerchia di operatori, consolidando il potere di chi è già potente, funzionerà da moltiplicatore e acceleratore delle disuguaglianze esistenti. In questo caso, la tecnica dietro un'apparente obiettività e neutralità avrà invece mortificato la sua potenziale capacità a ridurre le ingiustizie.

Il contributo di Marco Orofino è dedicato alla tutela dei dati personali nel settore delle comunicazioni elettroniche e alla crisi del modello settoriale adottato dall'Unione europea con l'approvazione, ormai risalente nel tempo, della Direttiva 2002/58/CE, cd. Direttiva *e-Privacy*. Un modello che prevedeva la configurazione della Direttiva in questione come *lex specialis* in un contesto in cui la *lex generalis* era la Direttiva "madre" 95/46/CE. L'Autore sottolinea come la trasformazione tecnologica (con l'emergere degli operatori OTT concorrenti con i tradizionali fornitori di servizi di comunicazione elettronica) e l'approvazione del GDPR, quale nuovo regolamento generale, abbiano reso tale modello inadeguato. La proposta – poi accantonata – di sostituire la Direttiva *e-Privacy* con un regolamento omonimo era il riflesso di tale obsolescenza. Negli ultimi anni, inoltre, l'Unione europea ha approvato numerosi regolamenti nel settore digitale (tra cui, a titolo esemplificativo, il *Digital Services Act*, il *Digital Markets Act*, il *Data Governance Act* e il *Data Act*), i quali hanno inciso in modo significativo sull'ecosistema delle comunicazioni e della gestione dei dati personali. L'insieme di tali interventi, pur orientati a disciplinare aspetti complementari del mercato digitale, ha reso ancora più evidente la necessità di intervenire nel settore delle comunicazioni elettroniche al fine di garantire un modello regolatorio coerente, sostenibile e capace di rispondere alle sfide tecnologiche presenti e future.

Un secondo gruppo di studi approfondisce le questioni emergenti nei mercati digitali con particolare attenzione al rapporto tra diritto della concorrenza e regolazione pro-concorrenziale. Allegra Canepa tratta in modo approfondito il tema delle piattaforme eco-

sistema, ossia piattaforme che aggregano servizi molto differenti tra di loro, regolamentati (come, ad esempio, quelli finanziari) e non (come l'ascolto della musica, il *video streaming*, etc.), suscettibili di guadagnare una posizione di forza sui mercati. Il contributo, in primo luogo, provvede a individuare quali siano le azioni di tali soggetti dirette ad aumentare la propria forza di mercato. In secondo luogo, verifica quali normative europee, primarie e secondarie, l'Unione europea possa utilizzare per contrastare questi fenomeni. L'attenzione è in particolare dedicata agli strumenti tipici del diritto antitrust europeo (e a una valutazione della loro efficacia nell'epoca delle piattaforme e degli ecosistemi digitali) e al recente Regolamento europeo sui mercati digitali, il quale, pur non essendo assimilabile a uno strumento di tutela della concorrenza, detta obblighi *ex ante* e asimmetrici a carico dei cd. *gatekeeper* al fine di contrastare quei comportamenti prodromici alla creazione di piattaforme ecosistema.

Stefania Serafini analizza il cambiamento, definito radicale nello scenario concorrenziale italiano, dovuto alla cessione da parte della TIM della sua rete fissa di telecomunicazione. Secondo la ricostruzione proposta, tale trasferimento ha le sue radici nella mutata strategia dell'Unione europea, che, con il Codice europeo delle comunicazioni elettroniche, ha rovesciato la sua storica posizione: da *service and access based competition* a *facilty based competition*. Il contributo, dopo aver ricostruito il processo che ha condotto allo scorporo e alla successiva cessione della rete, prende in esame gli effetti della cessione su due soggetti. L'Autrice guarda alla posizione della società acquirente Fibercop, operatore *wholesale only*, come tale, sottoposto agli specifici obblighi regolamentari propri dei mercati dell'accesso all'ingrosso; ma pure al cessionario TIM, che ha reclamato una revisione degli obblighi normativi originari a seguito dell'avvenuto scorporo della rete. Le conclusioni sono dedicate agli scenari futuri e alle possibili innovazioni, che l'UE si accinge ad apportare al Codice europeo delle comunicazioni elettroniche.

Il contributo di Maria Francesca De Tullio indaga intorno alle trasformazioni dell'equilibrio tra innovazione, autodeterminazione informativa e concorrenza, che sembrerebbero compiersi con la recente normativa europea in tema di *big data*. L'Autrice pone parti-

colare attenzione al ruolo della geopolitica in tale rivisitazione di concetti cardine, come quello della concorrenza. La tesi di fondo è che la concorrenza non si riduce a una normativa tecnica, perché essa rimanda a scelte politiche fondamentali che necessariamente la precedono e poi la guidano. Il saggio individua tra le *political issues*: la sovranità digitale, la sicurezza e il rispetto dei diritti fondamentali, come emerse nella più recente normativa europea sulla società digitale.

Il tema della sovranità tecnologica e del rapporto tra regolazione dei mercati e sicurezza in chiave geopolitica è altresì oggetto del contributo di Andrea Ruffo, che esamina l'approccio dell'Unione europea alle tecnologie critiche, ossia, come precisa l'Autore, a quell'insieme di beni, conoscenze e infrastrutture digitali la cui disponibilità, integrità e sicurezza sono fondamentali per la sopravvivenza di uno Stato, inteso unitariamente come entità politica, economica e strategica. Il contributo mette in evidenza le due gambe della filosofia europea: il potenziamento dei centri di competenza e dei partenariati industriali, e l'attenzione alle nuove forme di regolazione. In questo senso sono centrali: la Direttiva NIS 2, il Regolamento (UE) 2019/452 che istituisce un quadro per il controllo degli investimenti esteri, il *Data Governance Act* e il *Digital Markets Act*.

Un terzo filone particolarmente fecondo dell'opera è dedicato ai diritti fondamentali e ai rischi emergenti nell'ambiente digitale.

Il saggio di Federico Gustavo Pizzetti affronta una delle frontiere più avanzate e delicate dell'innovazione contemporanea, analizzando gli effetti che le neuro-tecnologie producono sul terreno dei diritti fondamentali. La ricostruzione ha specificamente a oggetto i neuro-dispositivi, il trattamento dei neuro-dati e l'impatto del loro utilizzo sulla dignità umana. Lo studio prende le mosse da un esame puntuale della "Raccomandazione dell'Unesco sull'Etica della Neurotecnologia", che costituisce il più aggiornato e ampio catalogo di regole giuridiche (ed etiche) per indirizzare gli Stati membri dell'Organizzazione internazionale nella regolazione dello sviluppo delle neurotecnologie e nel trattamento dei neuro-dati. Esso prosegue analizzando la compatibilità delle norme primarie e secondarie adottate dall'Unione europea rispetto alle raccomanda-

zioni dell'Unesco. Specifica attenzione è dedicata, tra le norme secondarie adottate dall'UE, al GDPR (che non contiene una definizione di neuro-dati), al Regolamento sui dispositivi medici e all'*AI Act*. Pregevoli le conclusioni, dove l'Autore sottolinea come la frammentazione delle norme europee in materia possa creare criticità nell'applicazione della Raccomandazione e quindi nella tutela dei diritti fondamentali, ma anche incidere negativamente sullo sviluppo di un mercato unico europeo dei neuro-dispositivi.

Chiara Galbersanini offre un'interessante ricostruzione di una particolare categoria di dati personali di carattere culturale. Come sottolinea l'Autrice, tali dati non godono oggi di una definizione espressa nel GDPR, con la conseguenza che la loro protezione oscilla tra quella garantita ai dati personali, in generale, e quella offerta ai dati personali speciali (cd. dati sensibili). Questo diverso regime incide, secondo la ricostruzione proposta, sulla protezione dell'identità personale e sulla sua corretta rappresentazione nello spazio digitale. Inoltre, proprio l'impossibilità di ricondurre tutti i dati personali di carattere culturale nell'ambito dei cd. dati sensibili aumenta la possibilità di profilazioni algoritmiche di tipo linguistico-culturali e, di conseguenza, il rischio di discriminazioni in danno di determinati segmenti sociali.

Un ultimo gruppo di saggi analizza le nuove dinamiche istituzionali della regolazione europea.

In quest'ottica il contributo di Lavinia Del Corona mette in luce, ricostruendone anche l'evoluzione nei diversi regolamenti, il progressivo accentramento di funzioni di esecuzione normativa – intesi sia come atti di esecuzione sia come atti delegati – nonché di amministrazione diretta in capo alla Commissione europea nella disciplina della società digitale. L'Autrice riflette in particolare su come questa tendenza al rafforzamento della Commissione europea incida oggi e, in un prossimo futuro, sul processo di integrazione europea.

Il tema della co-regolazione è oggetto della riflessione di Antonio Foti, che attraverso la metafora della "sfera di Hoberman" restituisce l'idea di uno spazio di autonomia lasciato ai privati, spazio questo, che – a seconda delle contingenze e degli obiettivi di volta in volta perseguiti dalla normativa europea – è suscettibile di espan-

dersi o ridursi. In quest'ottica, l'Autore analizza i principali regolamenti dell'Unione europea, distinguendo una co-regolazione "a maglie larghe" da una "a maglie strette", in ragione dello spazio disponibile ai privati.

Completa la raccolta il contributo di Fulvia Abbondante, dedicato alla regolazione delle telecomunicazioni e alla *data protection* nel Regno Unito, prima e dopo la *Brexit*. L'esame delle innovazioni introdotte (o tentate) dal Regno Unito offre certamente uno sguardo comparato, ma soprattutto arricchisce la prospettiva europea. Di particolare interesse, per i temi oggetto di questo lavoro, sono alcune delle soluzioni sperimentate in tema di neutralità della rete, di accesso e uso dei dati, nonché la più generale tendenza a una convergenza regolatoria tra telecomunicazioni e dati personali.

Nel loro insieme, questi saggi mostrano come la trasformazione digitale richieda nuovi strumenti giuridici, nuove categorie concettuali e, soprattutto, un criterio interpretativo *constitutional by design*, in grado di tenere insieme diritti, tecnica e mercati. Il volume vuole essere, non una semplice raccolta di studi, ma un'opera corale, ambiziosa nell'orientare il dibattito pubblico e accademico su temi destinati a incidere profondamente sulla vita dell'Europa e dei suoi cittadini.

Siamo grati agli Autori e a quanti hanno contribuito a dilatare i nostri orizzonti specialistici e, prima fra tutti, alla coordinatrice del Progetto *Net4Future*, Ilenia Tinnirello.

Da questo incontro tra diritto e tecnica è nata una tensione a uscire dai confini settoriali e a esercitarci in una lettura del processo economico-sociale, che, nato in basso, prova a disegnare modelli regolatori aderenti alla sua genesi. Questi modelli non sono camicie di forza, ma abiti cuciti su un divenire fenomenico, che va rispettato nella sua identità mutevole, ma anche orientato verso l'obiettivo dell'uguaglianza, secondo la tensione del costituzionalismo comune, che rivendica la prevalenza della scienza della qualità, la Politica, su quella della quantità, la Tecnica.

*Giovanna De Minico* e *Marco Orofino*

GIOVANNA DE MINICO

# REGOLE O LIBERTÀ PER LE TELECOMUNICAZIONI DEL FUTURO?

SOMMARIO: 1. L'attenzione al passato. – 2. Telco e *Gatekeeper*: uguali nelle funzioni. – 3. Telco e *Gatekeeper*: diversi nelle regole. – 3.1. La gestione degli *asset*. – 3.2. Il *fair share*. – 4. Quale (de)regolazione? – 5. L'attenzione al futuro.

## 1. *L'attenzione al passato*

Il mercato delle telecomunicazioni è stato ridisegnato nel tempo da interventi eteronomi e sovranazionali, che hanno determinato un'inversione di rotta dell'originaria tendenza: da un'offerta concentrata in un unico operatore pubblico a una diffusa e tendenzialmente privata. Da qui l'orientamento del mercato in principio monopolistico in direzione di una competizione protetta. Le forze sinergiche della liberalizzazione e della privatizzazione non riuscirono però ad aprire il mercato ai nuovi *competitors*, in quanto l'ex monopolista continuava a detenere una posizione di vantaggio strutturale[1], ostacolo all'ingresso di forze concorrenti. Il vantaggio dell'*incumbent* era dovuto alla sua identità di operatore verticalmente integrato, cioè presente sul mercato all'ingrosso (come gestore di rete) come su quello al dettaglio (come fornitore del servizio), il che costringeva i concorrenti a rivolgersi a lui per negoziare gli *input* di rete, indispensabili a prestare il servizio al cliente finale.

Queste carenze strutturali del mercato rendevano necessario l'intervento di una regolazione asimmetrica: "preconditions of a

[1] S. FROVA, E. PONTAROLLO (a cura di), *La liberalizzazione zoppa. Il caso della telefonia fissa*, Milano, 2004, p. 35 ss.

competitive marketplace rather than substituting regulation for competition, (…) Necessary when antitrust cannot successfully maintain a workably competitive market place (…)"[2]. Questa, senza pretesa di sostituirsi alla *competition law*, sarebbe stata in grado di fare quanto la seconda non avrebbe potuto: cioè, riequilibrare la diversità delle posizioni iniziali tra imprenditori. La norma asimmetrica si qualificava per il metodo impiegato per correggere i fallimenti di mercato, imponendo un rapporto obbligatorio a senso unico, dove l'*incumbent* era tenuto a concludere contratti di uso della sua struttura aziendale a favore dei neocompetitori alle medesime condizioni riservate alle proprie divisioni commerciali, assorbendo di fatto lo spazio riservato all'autonomia negoziale in nome dell'uguaglianza sostanziale, principio ordinatorio, non dei soli diritti sociali, ma anche delle libertà economiche. Questo intervento eteronomo e conformativo dell'autonomia negoziale avrebbe mimato un mercato concorrenziale, creando con *fictio iuris* condizioni analoghe a quelle che un mercato competitivo produrrebbe naturalmente, in modo da consentire alle nuove imprese l'accesso alla rete dell'ex monopolista.

La disciplina asimmetrica era in un rapporto di complementarità con quella *antitrust*, da cui manteneva una sua autonomia di identità per ciò che riguarda i fini. Infatti, l'obiettivo della normativa asimmetrica è promuovere l'economia di libero scambio, simulando le condizioni strutturali di un mercato maturo: il suo sguardo è dunque rivolto al futuro perché gioca al rialzo. Al contrario, la disciplina *antitrust* mira a preservare lo stadio competitivo raggiunto, cioè gioca una partita conservativa. Ne consegue che la normativa asimmetrica si applica per prevenire un probabile abuso (opera *ex ante*), perfezionandosi al verificarsi di una situazione di pericolo per la competizione. Tale è la presenza sul mercato di un ex monopolista in posizione dominante, il cui potere di mercato viene trattato come se fosse un 'male in sé' secondo un giudizio di prognosi *ex ante*. In altri termini, la disciplina asimmetrica non scommette sulla

[2] In proposito, cfr.: S. BREYER, *Regulation and its reform*, Cambridge, 1982, pp. 158-159; ID., *Antitrust, deregulation and the newly liberated marketplace*, in *Cal. L. Rev.*, 75, 1987, p. 1007.

buona fede dell'imprenditore perché parte dal timore che il potere personale sia incline a subire una deriva egoistica[3].

L'*antitrust*, invece, opera *ex post* e ha carattere repressivo, intervenendo a violazione consumata per rimuovere l'illecito e ripristinare la situazione di concorrenza pregressa. In sintesi, la regolazione asimmetrica crea le condizioni di effettività della normativa *antitrust*, la cui applicazione diviene dunque residuale. Il rapporto tra le due discipline si traduce nel modello matematico della proporzionalità inversa, per cui un mercato caratterizzato da forte insufficienza competitiva richiederà un apporto massiccio di disciplina correttiva, destinato a decrescere e infine ad azzerarsi al crescere della competizione.

Su questo impianto concettuale sono intervenuti i Pacchetti Direttive 2002 e 2009, nonché il Codice delle Comunicazioni elettroniche[4], che hanno segnato la fine della normativa asimmetrica di prima generazione. Quest'ultima era collegata al 'peccato originale'[5]

---

[3] L.J.H.F. GARZANITI, *Telecommunications, Broadcasting and the Internet: EU competition Law and regulation*, Sweet & Maxwell, 2003, 2ª ed., p. 539: "They have been adopted on the assumption that market forces alone, even under the threat of *ex post* application of competition rules, would not suffice, at least not in the short term, to achieve a fully competitive market given that at liberalisation, incumbent operators had monopoly or very strong market position. In this sense, sector-specific rules complement the competition rules". Anche: I. WALDEN, J. ANGEL, *Telecommunications law and regulation*, Oxford, 2005, p. 322 ss. Ancora si veda: P. NIHOUL, P. RODFORD, *EU electronic communications law*, Oxford, 2004, pp. 18-19.

[4] Decreto legislativo del 1° agosto 2003, n. 259, di recepimento delle direttive 2002/19/CE (Direttiva accesso), 2002/20/CE (Direttiva autorizzazioni), 2002/21/CE (Direttiva quadro) e 2002/22/CE (Direttiva servizio universale), recante il "Codice delle comunicazioni elettroniche" (Codice C.E.), in G.U. n. 214 del 15 settembre 2003. Il primo pacchetto è stato successivamente modificato dalla Direttiva 2009/136/CE, del 25 novembre 2009; e da ultimo: Direttiva (UE) 2018/72, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche.

[5] L'espressione si deve a A. DE STEEL, *Remedies in the European electronic communications sector*, in D. GERADIN (ed.), *Remedies in Network Industries: EC competition law vs. sector-specific regulation*, in *Intersentia*, 2004, a p. 31, dove l'Autore afferma che "Under the 1998 framework, the SMP regime was mainly related to the competitive conditions under which infrastructures have been deployed. It mainly applied to markets previously under legal monopoly […] and was thus linked to the so-called original sin of the previous monopolist". In proposito, anche: P. LAROUCHE, *A closer look at some assumptions underlying EC regulation of electronic communications*, in *Jour. of network industries*, 3, 2002, p. 141.

dell'ex monopolista, la cui situazione di vantaggio era considerata un pericolo in sé per la *par condicio* competitiva. Di conseguenza, la fattispecie asimmetrica si risolveva in valutazioni legali tipiche, previsioni di dominanza *ex ante* immodificabili e imposizioni integrali delle misure correttive.

Con i Pacchetti Direttive 2002, 2009 e il relativo Codice C.E. il processo normativo ha conosciuto un nuovo fuoco: la necessità di valutare i mercati secondo il loro divenire storico. Il cambiamento di prospettiva ha reso le nuove regole correttive più sofisticate nei presupposti, modulabili nei contenuti e temporanee nella durata. Alle valutazioni predeterminate dal legislatore comunitario si sono sostituiti gli accertamenti sul campo rimessi alle Autorità Nazionali di Regolazione (ANR), che selezionavano i mercati secondo le rispettive specificità e in linea con i principi del diritto *antitrust*. L'esito della selezione era affidato ora a un test a tre punte: esso valutava l'esistenza di barriere all'accesso forti e non transitorie, l'assenza prospettica di competizione effettiva e l'insufficienza della sola legge *antitrust* a sanare le disfunzioni. Questo approccio pragmatico aveva il pregio di evitare il rapido invecchiamento dei mercati, giudicandoli dal punto di vista della concorrenza dinamica. Analogamente, l'operatore con significativo potere di mercato, non più individuabile *ex lege* in ragione della soglia di fatturato, era accertabile *ex post* dalle ANR in virtù dei criteri tecnico-economici elaborati dalla Commissione e dalla Corte di giustizia in tema di posizione dominante[6]. Infine, i rimedi, non più applicabili in blocco, erano ora rimessi alla selezione delle ANR in vista della misura più appropriata e proporzionata alla disfunzione da correggere. L'obiettivo programmatico della disciplina asimmetrica europea era avviare un flusso normativo snello, composto da regole asimmetriche decrescenti e sofisticato nella tecnica di formulazione perché basata su analisi complesse, causa di *rule-making* diluiti nel tempo. Ma al di là dell'annunciata vocazione flessibile, l'azione della Commissione tendeva invece a blindare il tessuto normativo con Direttive e

[6] R. Wish Bailey, *Competition law*, Oxford, OUP, 2018, capp. 17 e 18; nonché, R. Nazzini, *The foundations of European Union of Competition law: The objective and principles of article 102*, Oxford, OUP, 2011, *passim.*

atti di *soft law* (in proposito si pensi alla Raccomandazione sui mercati rilevanti[7], interpretata dalle ANR come una presunzione assoluta e inderogabile).

Questo atteggiamento iper-regolatorio ostacolò l'alleggerimento normativo[8] promesso, fino ad assorbire l'individuazione del mercato rilevante e dell'operatore con *Significant Market Power* (SMP) in un unico *step*, che con moto centripeto si affrettava a concentrare compiti e funzioni nell'Esecutivo sovranazionale, mortificando l'intenzione di devolvere alle ANR maggiore discrezionalità tecnica, come pure il principio di sussidiarietà avrebbe richiesto.

Anche l'implementazione nazionale contribuì a blindare il corpo normativo, ne sia prova la circostanza che le ANR, inclusa l'Ag.Com. italiana, scelsero prevalentemente i rimedi comportamentali: l'obbligo legale a contrarre e il principio di non discriminazione con il corollario della parità di trattamento interno/esterno. Tale opzione aveva trascurato la possibilità, pur prevista in circostanze eccezionali dall'art. 8, par. 3, della Direttiva Accesso, di ricorrere a misure strutturali atipiche, quali la separazione societaria o proprietaria, le sole ritenute idonee a neutralizzare efficacemente il conflitto di interessi fisiologico dell'operatore verticalmente integrato.

In sintesi, i soli rimedi comportamentali si sono rivelati inadeguati a prevenire gli illeciti concorrenziali, in quanto l'*incumbent*, pur rispettando formalmente la disciplina, continuava indisturbatamente ad abusare delle sinergie tra gestione di rete e fornitura di servizi, riservando condizioni deteriori ai suoi concorrenti. La prova definitiva dell'inefficacia delle misure preventive era dunque nei reiterati abusi di posizione dominante dell'*incumbent*, a conferma del fatto che un mercato concorrenziale non si poteva creare a tavolino con le sole regole asimmetriche, peraltro addomesticate.

---

[7] Cfr. la Raccomandazione della Commissione del 11 febbraio 2003, in part. il Cons. 9.

[8] Già nel 2006 la Commissione inseguiva la *lighter regulation - Communication on Market Reviews under the EU Regulatory Framework*, COM (2006), 28 *final*, a p. 10, *http://europa.eu.int/information_society/policy/* come si insegue un mito, il quale quando sta per avverarsi si allontana. Poi nel 2025 l'alleggerimento normativo diventa l'obiettivo primario nel *Digital Networks Act*, ma di ciò parleremo nel prosieguo del lavoro.

## 2. *Telco e* Gatekeeper*: uguali nelle funzioni*

L'evoluzione strutturale e funzionale dei mercati TLC, parte dell'ecosistema digitale, ha dimostrato che equiordinare gli operatori di TLC non sarebbe bastato per conseguire l'obiettivo uguaglianza perché l'originaria distinzione tra i titolari dell'infrastruttura di rete e gli *other licensed operators* (coloro che ne sono privi) è sostituita da una nuova relazione disallineata: quella che corre tra gli operatori di TLC e coloro che prestano attività analoghe alla comunicazione elettronica, ma con mezzi alternativi alle reti fisse o mobili. In proposito, si pensi al trasporto della voce su *Internet* equiparabile funzionalmente alla telefonata su rete Telco. Questa discontinuità nei mezzi, non anche nella prestazione, ha come protagonisti i *Gatekeeper* (GK), che offrono al cittadino-utente l'intero pacchetto dei servizi della *E-society*, tramite *Internet*; rete, questa, che a sua volta necessita di un'infrastruttura fisica di connettività, fornita dalle Telco. Pertanto, i GK si comportano nei confronti delle Telco come quell'uccello che, deposte le uova nel nido altrui, lascia che sia un altro a covargliele; in modo analogo i GK si servono delle infrastrutture di rete – bene di proprietà delle Telco – senza assumersi i relativi costi di realizzazione e di mantenimento.

Quindi, il diritto sovranazionale, preso atto di questa disparità, invece di rimuoverla, la legittima con norme giuridiche che dispongono trattamenti differenziati per operatori funzionalmente equiordinati; alla fine del gioco regolatorio le condizioni di concorrenza tra imprenditori, che vendono beni e servizi su mercati distinti, ma reciprocamente interdipendenti, sono irrimediabilmente alterate perché non sono collocati sul medesimo piano di gioco.

Davanti a questo quadro economico e normativo inedito, che andava compreso nella sua intima sostanza, la Commissione europea invece imposta il discorso regolatorio partendo da una visione formalistica degli attori in gioco e pertanto li distingue a seconda che operino sul mercato delle TLC o su quelli digitali in ragione di una diversità solo formale dei servizi rispettivamente procurati. L'Esecutivo europeo non vede che questi soggetti, diversi per identità, tornano a coincidere nelle prestazioni offerte all'utente finale, come l'esempio della VoIP prima illustrato insegna che una telefonata rimane tale a prescindere dal mezzo di trasmissione.

Il ragionamento della Commissione porta a giustificare l'ingiustificabile: un'odiosa asimmetria regolatoria tra Telco e GK, impeditiva dell'uguaglianza orizzontale, tanto all'interno del settore delle telecomunicazioni, quanto nei rapporti tra quest'ultimo e gli operatori digitali. Vediamo allora se esistono e quali sono i possibili strumenti regolatori capaci di colmare i *vulnera* all'uguaglianza.

Questa sarà l'ottica di lettura del Rapporto Draghi[9], che da un lato coglie i *defeat* del mercato delle telecomunicazioni; dall'altro, mette in luce l'intreccio profondo, dovuto alla convergenza tecnologica, che lega il mercato TLC alle piazze digitali. Quanto al primo profilo, il Rapporto attribuisce il ritardo tecnologico dell'UE a un'eccessiva frammentazione dell'offerta, appunto caratterizzata dalla presenza di piccoli e numerosi operatori, incapaci pertanto di investimenti cospicui in *Research & Innovation* (R&I)[10], anche a causa dell'elevato prezzo delle aste per le frequenze (es. quelle del 5G), che arricchiscono il concessionario pubblico e impoveriscono il concedente al punto da non permettergli di investire nelle reti a copertura totale, a bassa latenza e veloci per veicolare la telemedicina e l'I.A.[11]. Di segno opposto è stata la politica industriale dell'UK, dove lo Stato si è accontentato di ricavi più modesti ma ha richiesto come controprestazione ai concessionari la loro collaborazione negli investimenti in reti, rispettando la vocazione sociale di questo bene e la sua natura incompatibile con il sotto-uso.

Secondo il Rapporto, tale polverizzazione sarebbe stata incentivata da un esubero regolatorio *ex ante*, nonché da politiche competitive che hanno ostacolato i processi di consolidamento a livello paneuropeo. Quindi, il prodursi di criticità strutturali che hanno impedito all'UE di sfruttare appieno il potenziale dei servizi digitali e delle tecnologie avanzate, con ripercussioni negative, non solo

---

[9] M. Draghi, *Il futuro della competitività europea*, 2024, in *https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059*.

[10] Ivi, *Il futuro della competitività europea*, in particolare, *Parte A - Una strategia di competitività per l'Europa*, pp. 27 ss., nonché *Parte B - Analisi approfondita e raccomandazioni*, pp. 72-74, 2024, in *https://commission.europa.eu/topics/competitiveness/draghi-report_en#paragraph_47059*.

[11] Queste le puntuali critiche di S. Cingolani, *Labriola ci spiega la crisi delle TLC, e come se ne può uscire*, in *Il Foglio*, 18 novembre 2025.

sulla digitalizzazione dei vari settori economici, quanto sulla competitività complessiva del sistema Europa[12].

Per superare l'inadeguatezza dell'attuale quadro normativo il Rapporto raccomanda di rivedere coraggiosamente l'approccio regolatorio, puntando su un unico mercato competitivo, quello delle Tecnologie dell'Informazione e della Comunicazione (TIC), che esige, se non unità, almeno equivalenza regolatoria, secondo la logica "stesse regole per stessi servizi"[13].

Questa equiordinazione normativa è strettamente connessa al secondo profilo indicato nel Rapporto: l'intreccio tra il mercato delle TLC e le piazze digitali data la richiamata convergenza tecnologica. Questa, infatti, ha spezzato la tradizionale corrispondenza biunivoca mezzo/servizio, perché il secondo termine di questa equazione ben può essere prestato da un mezzo diverso da quello inizialmente deputato[14], riproponendo sul piano dei traffici economici quanto da tempo era già accaduto sul terreno dei rapporti istituzionali, dove, saltata la corrispondenza potere pubblico e funzione, una medesima funzione poteva essere esercitata da poteri diversi da quelli inizialmente riservatari della stessa.

L'analisi è matura per una domanda: quali sono le conseguenze di questo divorzio del mezzo dal servizio?

## 3. *Telco e* Gatekeeper*: diversi nelle regole*

Il Regolamento 2022/1925, *Digital Markets Act*[15], sarà il nostro banco di prova, e lo leggeremo diviso in due ideali colonne: da un lato, la disciplina dedicata alle Telco; dall'altro, quella rivolta ai GK al fine di valutare se le regole indirizzate ai GK pesino quanto quelle imposte alle Telco.

---

[12] M. Draghi, cit., p. 27: "Il conseguente ciclo di scarso dinamismo industriale, bassa innovazione, bassi investimenti e bassa crescita della produttività in Europa è stato definito "la trappola della tecnologia intermedia"". Cfr. D. Hanzl-Weiss, & R. Stehrer, *Dynamics of productive investment and gaps between the United States and EU Countries*, in *European Investment Bank Economics Working Paper*, 1, 2024.

[13] M. Draghi, *Il futuro della competitività europea, Parte B - Analisi approfondita e raccomandazioni*, cit., p. 81.

[14] Ivi, pp. 72-74.

[15] Regolamento (UE) 2022/1925, *Digital Markets Act* (DMA), la letteratura è sterminata, ma qui si rinvia ai soli Autori funzionali al nostro ragionamento.

Esiste un comune terreno tra i due corpi normativi in esame: la natura asimmetrica. Entrambi sono infatti concepiti per congelare una posizione di dominanza: rispettivamente, degli operatori verticalmente integrati e dei GK per evitare che la stessa degeneri in abuso. Messo da parte l'attributo teleologico, il resto delle due *regulation* presenta però più differenze che punti in comune.

Innanzitutto, si pone una questione di metodo. Invero, la disciplina TLC esige un'indagine sul piano fattuale di tre elementi: i mercati rilevanti, la condizione di dominanza dell'operatore e il grado di competizione attuale o potenziale del mercato come individuato. Questa pragmaticità nel metodo è mutuata dalla *lex mercatoria*, che, continuando a fare da modello, non assume questi elementi come ricorrenti *in re ipsa*, ma li accerta nel loro concreto verificarsi, e, solo dopo, assegna loro la qualifica più *suited and tailored* alla specificità delle situazioni, individuando i rimedi più consoni ma entro la rosa di quelli preindicati dalla legge. Invece, la disciplina del DMA identifica l'impresa dominante e i mercati digitali sulla base di indici presuntivi, saltando con disinvoltura la fase dell'accertamento dei fatti, assumendoli secondo una valutazione legale tipica.

Invero, una società è ritenuta GK in presenza delle seguenti condizioni: *a*) esercizio di influenza rilevante sul mercato interno; *b*) prestazione di un servizio di *trait d'union* tra l'offerta di servizi digitali e la loro domanda da parte dei consumatori finali; e *c*) esistenza stabile e in prospettiva duratura del dominante (art. 3, co. 1, DMA). Sebbene tali condizioni richiederebbero una verifica fattuale, si considerano invece automaticamente soddisfatte se la piattaforma superi le soglie quantitative del volume d'affari e del numero di utenti (art. 3, co. 2, DMA).

La prova della natura astratta del criterio è confermata dalla circostanza che gli obblighi imposti ai GK (*ex* artt. 5 e 6, DMA) si applicano indipendentemente dalla verifica di tre elementi: grado di concorrenzialità del mercato, posizione dominante e danno effettivo ai consumatori[16]. Ne deriva che tali regole risultano particolar-

[16] P. Ibáñez Colomo, *The Draft Digital Markets Act: a Legal and Institutional Analysis*, in *Journal of European Competition Law & Practice* 7, 2021, p. 571.

mente gravose e odiose agli operatori designati GK, perché impongono loro costi sproporzionati e soprattutto inutilmente pervasivi sull'autonomia imprenditoriale. Infatti, tali regole, applicandosi a prescindere dal grado di contendibilità del mercato, non contribuiscono ad ampliare le possibilità di accesso a favore di operatori potenziali perché il mercato potrebbe in ipotesi essere già naturalmente contendibile e quindi non avere bisogno di nessuna regola che lo elasticizzi forzosamente.

Il medesimo eccesso di astrattezza lo ritroviamo sul piano temporale, a conferma della distanza dal modello Telco: si indebolisce il rapporto di proporzionalità inversa tra le regole asimmetriche e la *Lex mercatoria*. Questo rapporto, quando funziona correttamente, comporta il ritiro progressivo delle regole asimmetriche all'avanzare della competitività del mercato; mentre nel DMA ciò non è contemplato. Infatti, anche quando un mercato raggiungesse il grado di equità e contendibilità auspicato dalla normativa, la revoca delle disposizioni normative rimarrà un evento futuro e incerto, salvo la previsione di una revisione triennale ad opera di una valutazione discrezionale della Commissione[17].

Ancora un eccesso di astrattezza si manifesta sul terreno dell'onere della prova e dell'individuazione dei rimedi. Nel settore delle telecomunicazioni spettava alle Autorità definire i mercati, individuare gli operatori dominanti e calibrare le misure; nel DMA è invece l'impresa stessa che, avendo superato le soglie quantitative, deve notificare alla Commissione la propria qualifica di GK e, qualora intenda sottrarsi a tale designazione, dimostrare di non rientrare nei criteri previsti[18]. In coerenza con questa linea, spetta inoltre all'impresa suggerire da sé come adeguare la sua condotta agli obblighi astratti di legge, assumendosi la responsabilità di individuare soluzioni adeguate, senza che la Commissione effettui una valutazione preventiva di proporzionalità.

È proprio l'assenza di un esplicito riferimento al principio di proporzionalità a marcare ulteriormente la distanza del DMA dal modello regolatorio TLC. Mentre quest'ultimo impone alle ANR di

[17] *Digital Markets Act*, art. 4, co. 3.
[18] Ivi, art. 3, co. 3 e co. 5.

scegliere sempre la soluzione meno invasiva, il DMA si limita a richiedere che le misure adottate siano "efficaci" (art. 8, co. 1), lasciando così intendere che interventi anche particolarmente incisivi siano legittimi purché idonei a conseguire lo scopo normativo[19].

A livello sistemico, il DMA – a differenza dei Pacchetti TLC prima esaminati – accetta di buon grado la sovrapposizione con il diritto antitrust, sebbene chiarisca che esso non mira a sostituirsi al diritto della concorrenza, ma solo a integrarlo (*Consideranda* 9 e 11 DMA), anche se tale distinzione ha il sapore di un'affermazione ostentata proprio per nascondere l'opposta realtà[20].

Il DMA riproduce infatti, nella sostanza e nella portata, gli obiettivi di equità e contendibilità propri del diritto antitrust[21]. Non sorprende, in questo senso, che l'elenco degli obblighi imposti ai GK coincida con la sintesi dei principali casi *antitrust* accaduti o ancora in corso[22]; da qui il sospetto che il DMA non rappresenti tanto una vera innovazione regolatoria quanto piuttosto una forma di "diritto della concorrenza settoriale" mascherato[23]. Le condotte vietate dal DMA – tra cui l'auto-preferenza, l'imposizione di clausole esclusive, l'obbligo di interoperabilità e la gestione congiunta dei dati – risultano ampiamente sovrapponibili a fattispecie poten-

---

[19] P. Ibáñez Colomo, *The Draft Digital Markets Act*, cit., p. 571.

[20] "Gli obiettivi generali dichiarati del regolamento DMA, ovvero equità e contestabilità, si sostanziano ai sensi dell'art. 10.2, nel divieto di comportamenti che implichino: *a*) uno squilibrio di diritti e obblighi sugli utenti aziendali, per mezzo del quale il *gatekeeper* ottiene dagli utenti aziendali un vantaggio sproporzionato rispetto al servizio a questi fornito; o *b*) una limitazione o indebolimento della contendibilità dei mercati. Equità e contestabilità, sia nella loro accezione generale, che come definite nel DMA (invero in modo piuttosto vago) non sono estranee alle politiche della concorrenza, ma parte integrante, a partire dalla relazione al DMA. In essa infatti si afferma che «le pratiche sleali e la mancanza di contendibilità creano inefficienze nel settore digitale in termini di prezzi più alti, qualità inferiore, minore scelta e minore innovazione, a scapito dei consumatori europei»" così: A. Manganelli, *Il regolamento Eu per i mercati digitali: ratio, criticità e prospettive di evoluzione*, in *Mercato Concorrenza Regole*, 3, 2021, pp. 489 ss.

[21] B. Beems, *The DMA in the broader regulatory landscape of the EU: an institutional perspective*, in *European Competition Journal*, 1, 2023, p. 6.

[22] C. Caffarra, F. Scott Morton, *The European Commission Digital Markets Act: A translation*, in *https://voxeu.org/article/european-commission-digital-markets-act-translation*, 2021.

[23] G. Colangelo, *DMA Begins*, in *Journal of Antitrust Enforcement*, 1, 2023, p. 4.

zialmente rilevanti ai sensi dell'art. 102 TFUE[24]. Questo genera un rischio concreto di duplicazioni investigative e di valutazioni divergenti, acuito dall'assenza di meccanismi dettagliati di coordinamento istituzionale.

Infine, si nota anche sul piano del contenuto il riproporsi dello squilibrio regolatorio tra Telco e GK, che invece ragioni di uguaglianza avrebbero dovuto escludere.

L'obbligo di base imposto alle Telco è consentire ai terzi l'accesso alla propria rete, come precedentemente illustrato. I GK non sono invece sottoposti ai sensi del DMA all'obbligo di *equal access*: Ad esempio, Amazon non deve accettare i prodotti che i fornitori gli chiedono di esporre sui suoi scaffali virtuali, ma, qualora decidesse di farlo, dovrà applicare le medesime condizioni riservate ai suoi venditori.

Chiediamoci se questa forte diversità regolatoria si giustifica in ragione di una diversità strutturale e funzionale dell'infrastruttura dei GK dalla rete fissa delle Telco.

Ebbene, entrambe le infrastrutture – virtuale e reale – sono essenziali per veicolare servizi ai cittadini. Riprendendo l'esempio precedente, Amazon fornisce a venditori e acquirenti uno scaffale digitale indispensabile per l'esposizione e quindi per l'acquisto dei beni; non diversamente da come le Telco forniscono una rete indispensabile alla comunicazione a distanza. Dal punto di vista sostanziale il risultato è identico: entrambi gli operatori mettono a disposizione mezzi necessari per prestare il servizio finale. Pertanto, questi mezzi – reti o piattaforme – dovrebbero essere sottratti alla disciplina privatistica, per essere attratti al diritto pubblico, senza però subire l'angusta qualifica di beni pubblici o di *essential facility*. A nostro avviso, essi compongono una categoria di beni ibridi, il che comporta la conseguente ibridazione della loro disciplina, che non potrà che essere pubblico-privata. Ad esempio, l'obbligo di consentire ai *competitor* di accedere alle proprie infrastrutture es-

[24] C. Fernández, *A New Kid on the Block: How Will Competition Law Get along with the DMA?*, in *Journal of European Competition Law & Practice* 4, 2021, p. 27; P. Akman, *Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, in *European Law Review*, 47, 2021, p. 2.

senziali andrebbe imposto alle Telco e ai GK; oppure rimosso a entrambi. Una proposta alternativa, sostenuta da alcuni studiosi[25], potrebbe essere quella di considerare i servizi digitali come *public utilities*[26]; lo scopo in ogni caso sarebbe quello di richiamare le grandi piattaforme nell'alveo del controllo pubblico con tutto ciò che ne seguirebbe in termini di eteronormazione quanto alla loro fisionomia e ai rispettivi poteri[27].

A differenza dei rimedi statici, quali le divisioni strutturali o aziendali, si potrebbero imporre doveri comportamentali, cioè dinamici: obblighi di accesso alla rete, di interoperabilità o di *sharing* di *cloud* pubblici. Ne conseguirebbe l'effetto di subordinare potenza e influenza delle *Big Tech* a scelte di *policy* pubbliche, che avrebbero titolo a ripensare la proprietà, il controllo e la *governance* delle infrastrutture digitali al fine di rendere aperto e contendibile il mercato digitale[28].

### 3.1. *La gestione degli* asset

Un'ulteriore differenza regolatoria tra Telco e GK si coglie nel tipo di disciplina, che regola gli *asset* alla base dei servizi erogati. La

---

[25] D. Schiller, *Reconstructing Public Utility Networks: A Program for Action*, in *International Journal of Communication* 14, 2020, p. 4989 ss.; J. Muldoon, *Don't Break Up Facebook - Make It a Public Utility*, in *Jacobin.com*, 2020, *https://jacobin.com/2020/12/facebook-big-tech-antitrust-social-network-data*; R.K. Sabeel, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, in *Georgetown Law and Technology Review*, 2, 2018, p. 246 ss. *https://ssrn.com/abstract=3220737*.

[26] La tradizione americana delle *public utilities* (risalente al diritto amministrativo del '900) attrae le piattaforme a una regolazione simile a quella delle imprese elettriche, ferroviarie o di telecomunicazioni, imponendo loro obblighi di: non discriminazione; accesso equo alle infrastrutture dati; limiti all'integrazione verticale dei servizi; *governance* trasparenti e funzionali all'interesse pubblico. Rifiutare la soluzione estrema di consegnare le piattaforme alla mano pubblica non impedisce di disegnare loro un regime giuridico *ad hoc*, che, in virtù della loro natura sociale, ne orienta le funzioni al *common good*.

[27] M. Zalnieriute, *Against Procedural Fetishism: A Call for a New Digital Constitution*, in *Indiana Journal of Global Legal Studies*, 2, 2023, p. 259.

[28] R.Griffin, *Public and Private Power in Social Media Governance: Multistakeholderism, the Rule of Law and Democratic Accountability, in public and private power in social media governance: multistakeholderism, the rule of law and democratic accountability*, in *Transnational Legal Theory*, 1, 2023 p. 4.

ricchezza dei GK trae origine dai dati degli utenti, conferiti con l'adesione negoziale alla piattaforma, dati questi, che, prima di essere utilizzati, sono organizzati, gerarchizzati ed elaborati al punto che il risultato finale sia un'entità qualitativamente diversa dalla somma matematica dei singoli elementi.

Se si considera la genesi di tali dati, in casi di abuso, la sanzione non può consistere nei rimedi tradizionali, bensì nella condivisione dei dati con quegli operatori, che, senza l'accesso all'*asset* essenziale, rimarrebbero ai margini di quel mercato.

A seguire la premessa scientifica di questo ragionamento, l'equiordinazione tra Telco e GK dovrebbe dunque suggerire una riflessione più ampia sull'intero sistema sanzionatorio, che dovrebbe mettere da parte le sanzioni pecuniarie o di *reductio in pristinum*, per rivolgersi a figure compensative in grado di neutralizzare le barriere tecnologiche con la condivisione parziale o integrale dei dati.

Tale esigenza deriva dalla lentezza dei procedimenti istruttori, che non stanno dietro al dinamismo dei mercati digitali, e dall'irreversibilità della lesione dei dati personali. In un tale contesto, il ricorso a strumenti negoziali, come gli impegni ai sensi dell'art. 9 del Reg. (CE) n. 1/2003[29], si rivela utile perché consente soluzioni rapide, flessibili e vincolanti per le parti coinvolte, favorendone la *compliance* e il ripristino della competizione, secondo criteri di ragionevolezza. La disciplina degli impegni può essere efficace tanto nel caso degli abusi di sfruttamento – quelli lesivi dei consumatori – quanto in quelli di esclusione – dannosi per i concorrenti.

Nel primo caso, condotte come la predisposizione di informative poco trasparenti o l'inserimento di clausole contrattuali squilibrate possono essere corrette dall'imposizione di obblighi di *disclosure* esterna[30] o mediante il riconoscimento del diritto alla portabi-

[29] Regolamento (CE) 1/2003 del Consiglio del 16 dicembre 2002 concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del Trattato, in *https://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX:32003R0001.*

[30] Il DMA, preso atto del crescente rapporto tra *privacy* e *antitrust*, prescrive una serie di obblighi che, pensati come strumenti di promozione della concorrenza, incidono direttamente sulla trasparenza delle pratiche digitali e sulla tutela dei dati personali. In particolare, due gruppi di norme risultano centrali: (*a*) quelle che limitano l'uso e la combinazione dei dati personali da parte dei *gatekeeper*; (*b*) quelle che raffor-

lità dei dati, restituendo così al consumatore l'autonomia decisionale[31] e stimolando la competizione al rialzo sulla tutela dei dati personali. Un simile approccio potrebbe, inoltre, ridurre il fenomeno del *lock-in*[32] e promuovere una maggiore contendibilità dei mercati digitali.

Occorre tuttavia rilevare che la *privacy* non è un bene "uniforme", soprattutto quando muta il suo terreno di giuoco dalla realtà analogica a quella digitale, terreno questo, rispetto al quale la sua consistenza e profondità si articola e misura[33] in base all'età, alla condizione economico-sociale, e alla disponibilità degli utenti a scambiare i propri dati dietro servizi digitali[34]. Gli impegni dovrebbero pertanto adottare una logica modulabile, prevedendo livelli differenziati di protezione, nel rispetto del principio di uguaglianza sostanziale[35].

---

zano la trasparenza dei processi di raccolta, utilizzo e condivisione dei dati (*infra*, nota 30). Per una comparazione della disciplina in materia di *privacy* tra GDPR e DMA quanto al consenso si veda: A.S. D'Amico, *The DMA's Consent Moment and its Relationship with the GDPR*, in *European Journal of Risk Regulation*, 16, 1, 2025, 170-183, *https://doi.org/10.1017/err.2024.38*.

[31] La portabilità dei dati è codificata nell'art. 6, par. 9, DMA, che impone ai *gatekeeper* di mettere a disposizione degli utenti finali (e di terzi da essi autorizzati) strumenti che garantiscano l'effettiva portabilità dei dati forniti o generati dall'attività dell'utente, incluso l'accesso continuo e in tempo reale. Si tratta di un ampliamento significativo rispetto al diritto alla portabilità previsto dall'art. 20 GDPR, limitato ai dati "forniti dall'interessato" e non assistito dagli obblighi tecnici di accesso costante. Sul punto: Centre on Regulation in Europe (CERRE), *Data Access, Interoperability and Portability in the Digital Markets Act*, 2022, 7 ss., *https://cerre.eu/wp-content/uploads/2022/11/DMA_DataAccessProvisions-2.pdf*.

[32] Per il DMA, in part. il Considerando 72: "Una maggiore trasparenza dovrebbe consentire alle altre imprese che forniscono servizi di piattaforma di base di differenziarsi meglio attraverso l'uso di maggiori garanzie della privacy." Mentre, la Commissione, *Google/Fitbit*, ha osservato che il GDPR non lascerebbe alcuno spazio a tale differenziazione in tema di privacy. Sul punto: P. Akman, *Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, cit., p. 2.

[33] Ampiamente argomenta sul concetto di una *privacy* a forma di prisma M. Orofino in questo *Volume*.

[34] Sul punto si vedano le pertinenti osservazioni di M.F. De Tullio in questo *Volume*.

[35] Quanto detto non risulta, tuttavia, esente da obiezioni perché le facoltà connesse a un diritto fondamentale potrebbero tradursi in uno *ius variandi* legato alla capacità economica del titolare.

Anche nel secondo caso – gli abusi di esclusione[36] – la condotta rimediale dovrebbe comportare misure di sharing dell'*asset*, perché al momento è l'unica capace di rimuovere le barriere tecnologiche all'entrata[37], ma anche di assicurare la contendibilità dei mercati. Essa andrebbe imposta, nonostante alcune criticità: come separare i dati suscettibili di comunione[38] da quelli che non lo sono; come sostenere gli investimenti e come superare le incertezze nella valutazione dell'*asset*.

Limitarsi all'irrogazione di sanzioni pecuniarie – approccio a lungo favorito dalla Commissione – non ricompone l'equilibrio competitivo originario, non orienta il mercato verso assetti diversi dai preesistenti, né previene le future condotte abusive[39].

---

[36] Si configura abuso escludente qualora si arrechi pregiudizio ai concorrenti, costringendoli a uscire dal mercato ovvero impedendo loro di accedervi. Cfr.: V. Kathuria, J. Globocnik, *Exclusionary Conduct in Data Driven Markets: Limitations of Data Sharing Remedy*, in *Journal of Antitrust Enforcement*, 8, 3, November 2020, 511-53.

[37] La concentrazione dei *Big Data* nelle mani di pochi, come ostacolo alla concorrenza, è uno dei punti di partenza del DMA. Infatti, nell'atto si riconosce che "i gatekeeper usufruiscono dell'accesso a grandi quantità di dati" e che questo potrebbe compromettere "la contendibilità dei servizi di piattaforma di base, o il potenziale di innovazione del dinamico settore digitale" (Considerando 59). La condivisione, pur non essendo esplicitamente prevista come rimedio, impone obblighi (seppur limitati) di *data sharing*: il *gatekeeper* deve garantire agli utenti commerciali (e ai terzi autorizzati da essi) l'accesso ai dati generati tramite le loro attività e quelle dei loro utenti finali (art. 6, par. 10); mentre, i motori di ricerca devono fornire dati relativi a posizionamento, ricerca, clic e visualizzazione (art. 6, par. 11). In proposito, cfr.: Centre on Regulation in Europe (CERRE), *Data Access, Interoperability and Portability in the Digital Markets Act*, 2022, cit., 5.

[38] M. Botta, K. Wiedemann, *Eu competition law enforcement vis à vis exploitative conducts in the data economy. Exploring the terra incognita, paper*, cit., *passim*; più di recente, cfr.: Id., *The Interaction of EU competition, consumer, and data protection. law in the digital economy: the regulatory dilemma in the Facebook odyssey*, in *The Antitrust Bulletin*, 2019, 64(3) 428-446.

[39] Il denaro ha una funzione deterrente del danaro solo se l'ammontare della pena pecuniaria sia superiore al guadagno illecito derivante dalla condotta vietata; nei mercati digitali, invece, i profitti da pratiche anticoncorrenziali – come l'auto-preferenza o l'imposizione di clausole esclusive – eccedono i massimali previsti dal DMA. Pertanto, le aziende preferiscono violare le regole e pagarne le sanzioni, assumendole come il "cost of doing business", piuttosto che conformarsi a normative che modificherebbero i redditizi modelli di business. Così: J. Espinoza, *Why Big Tech fines don't work*, in *Financial Times*, 10.4.2024, *https://www.ft.com/content/ba6eb664-b981-42d7-b24a-65e7e19889f8*; W. Streeter, *How Tech Giants Absorb Penalties with Ease*, in *londonlovesbusiness.com*, 5.4.2024, *https://londonlovesbusiness.com/how-tech-giants-ab-*

Adottando invece la prospettiva dello *sharing* aziendale, si compirebbe il passaggio dai rimedi comportamentali a quelli strutturali, fondati sulla comproprietà o sul co-uso dell'*asset*, che, pur previsti sia dall'art. 7 del Reg. (CE) n. 1/2003 che dall'art. 18 del DMA[40], sono tuttavia concepiti in *extrema ratio*, adottabili solo se le misure comportamentali siano inefficaci o più onerose, secondo i principi di proporzionalità e necessità.

In alternativa, può rendersi opportuna la cessione coattiva di servizi o rami d'azienda del dominante, al fine di ridurre l'integrazione verticale e favorire la competitività[41].

---

*sorb-penalties-with-ease*; A. Ezrachi, M.E. Stucke, *How Big-Tech Barons Smash Innovation - And How to Strike Back*, NY, Harper Business, 2022, 10: "Although nearly all the Tech Barons are being sued across several jurisdictions, they have little to fear".

[40] L'art. 18 DMA prevede l'ipotesi – soggetta a stringenti requisiti – che, in caso di inosservanza reiterata, la Commissione possa imporre "qualsiasi rimedio comportamentale o strutturale proporzionato e necessario per garantire l'effettivo rispetto del regolamento", tra cui – a titolo esemplificativo – il divieto temporaneo per il *gatekeeper* di compiere operazioni di concentrazione. Se, da un lato, questa previsione potrebbe funzionare da deterrente (cfr.: A. D'Amico, A. Gerbrandy, *Breaking up the Tech-Giants, for Real?*, in *Kluwer Competition Law Blog*, 29.1.2025, *https://legalblogs.wolterskluwer.com/competition-blog/breaking-up-the-tech-giants-for-real/*); dall'altro, come sanzione indefinita nel *quomodo* genera incertezza giuridica, il che potrebbe disincentivare l'innovazione tecnologica perché l'atto si presterebbe a facili impugnative dinanzi al giudice.

[41] Interessante, in tal senso, anche la cessione coattiva richiesta nella causa intentata dal *Department of Justice* contro Google 2020: il governo ha chiesto al giudice, come misura correttiva, di ordinare la separazione di alcune parti del *business* di Google. Specificamente, il DOJ vuole che Google divida/separi Chrome (il suo *browser*) e/o Android (il sistema operativo mobile) dal suo motore di ricerca o che comunque venda alcune parti, al fine di ridurre la leva che Google ha sulle infrastrutture "di default" (dispositivi, *browser*), che favoriscono la sua ricerca. La richiesta non è stata accolta (United States v. Google LLC, 2 settembre 2025); il giudice Amit P. Mehta si è rivelato tendenzialmente adesivo alle argomentazioni di Google, ritenendo che tali rimedi strutturali sarebbero "radicali", rischiosi, e non pienamente giustificati dal peso del danno dimostrato, anche in considerazione del fatto che Google Search vedrà attenuata la sua dominanza nel campo della ricerca online dai modelli di ChatGPT in grado di fare ricerche anche migliori nelle prestazioni da quelle dello storico rivale. Sono stati invece imposti rimedi comportamentali, quali la cessazione di accordi esclusivi (la vendita di servizi necessariamente in "pacchetto") e l'obbligo di condividere con concorrenti qualificati in parte sia i dati indicizzati della ricerca ("search index") che quelli di interazione con gli utenti ("user-interaction data"). In merito si vedano: E. Dans, *Antitrust as bad joke: Google dictates its own sentence*, in *Medium.com*, 5.9.2025, *https://medium.com/enrique-dans/antitrust-as-bad-joke-google-dictates-its-own-sentence-581b377db5d9*; E. Dou, *Judge bars Google from exclusive search deals but*

Un esempio di adozione di rimedi strutturali, in luogo dei tradizionali rimedi comportamentali, si è realizzato nel recente caso *Google AdTech*. La Commissione europea ha ordinato a Google – colpevole di autopromuovere i propri servizi di pubblicità *online* – non solo di porre fine a tale condotta abusiva, ma anche "to cease its inherent conflicts of interest along the adtech supply chain"[42]. Lasciare a Google la possibilità di proporre il rimedio strutturale, anziché imporglielo direttamente, non ne cambia la sostanza perché il provvedimento mira, seppur indirettamente, a conformare la condotta e l'organizzazione dell'impresa digitale *pro futuro*[43].

L'adozione di impegni 'su misura' consente di evitare l'automatica applicazione di rimedi di *privacy-based* o, al contrario, di trascurare l'incidenza delle violazioni *antitrust* sulla protezione dei dati, imponendo invece un metodo di lavoro aderente alla pluriffensività dell'illecito e disponibile a soluzioni aderenti[44] alla specificità dei fatti; insomma, un *case by case* ritagliato sulla natura dell'illecito. L'evoluzione della prassi della Commissione europea nella valutazione degli illeciti *antitrust* della *e-economy* mostra, così, un approccio tecnicamente orientato, capace di modulare le figure di illecito in funzione del dinamismo dei mercati digitali, lasciando invariate le norme sostanziali.

Ritornando alle nostre Telco, anche questi soggetti possano essere obbligati a dividere la rete? Sebbene l'obbligo non sia mai

---

*says it can keep Chrome*, in *The Washington Post*, 2.9.2025, *https://www.washingtonpost.com/technology/2025/09/02/google-search-monopoly-antitrust-remedy/*.

[42] European Commission, *Press release, Google AdTech 2025 (AT40670), 5 September 2025*, in *https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1992.*

[43] European Commission, *Press release, Google AdTech 2025 (AT40670)*, cit.: "Where the Commission finds that there is an infringement of Article 102 of the TFEU, it may by decision require the company concerned to bring such infringement to an end. For this purpose, it may impose on them any behavioural or structural remedies which are proportionate to the infringement committed and necessary to bring the infringement effectively to an end. Structural remedies can only be imposed either where there is no equally effective behavioural remedy or where any equally effective behavioural remedy would be more burdensome for the company concerned than the structural remedy".

[44] Pertanto, anche le Autorità dovrebbero operare in modo coordinato, distinguendo tra competenza principale e quella accessoria, per cui spetterà all'Autorità Antitrust la decisione finale, mentre all'Autorità per la protezione dei dati personali il potere di intervenire nel procedimento principale con un parere obbligatorio.

stato effettivamente ordinato, in punto di diritto la sanzione non si potrebbe escludere, stante la previsione di legge. Ne consegue che in linea di principio le Telco potrebbero essere costrette alla scissione proprietaria della rete, perché un'infrastruttura essenziale per assicurare l'accesso al mercato dei futuri concorrenti, parallelamente i dati detenuti dai GK potrebbero essere oggetto di una condivisione forzosa totale o parziale con i GK entranti, per attenuarne la dimensione verticalmente integrata, sopra esaminata.

In sintesi, è tempo di un intervento regolatorio pubblico che disegni un quadro di norme omogenee, che, senza trascurare le peculiarità soggettive dei diversi operatori, introduca norme e modelli di comportamento in linea con le rispettive posizioni di mercato e tenute al minimo indispensabile per la contendibilità delle piazze digitali ai terzi aspiranti, privi di infrastrutture, ai dati o alle reti.

### 3.2. *Il* fair share

Il difetto di un siffatto allineamento regolatorio quanto all'*equal access* e alla gestione degli *asset* rischia di consolidare un indebito vantaggio competitivo in favore dei GK, di cui si intravede un forte indizio nella loro mancata partecipazione agli oneri di investimento nelle reti di nuova generazione.

In ragione di ciò, gli operatori di telecomunicazioni chiedono alle Autorità UE di introdurre un obbligo di *fair share* a carico delle grandi piattaforme digitali[45]. L'obiettivo è garantire che i GK, che traggono i maggiori benefici dalle infrastrutture di rete, contribuiscano ai 174 miliardi di dollari necessari, secondo le stime della Commissione, a raggiungere i "target di connettività del 2030" previsti dal programma *Digital Decade 2030*[46], cifra questa, che il solo settore delle telecomunicazioni non potrebbe raggiungere senza apporti altrui.

---

[45] P. Licata, *Fair Share: 20 Telco in pressing, basta asimmetrie: le Big Tech devono contribuire alle reti*, in *corrierecomunicazioni.it*, 2.10.2023, *https://www.corrierecomunicazioni.it/telco/fair-share-20-telco-in-pressing-basta-asimmetrie-le-big-tech-devono-contribuire-alle-reti/*.

[46] WIK-Consult, *Investment and funding needs for the Digital Decade connectivity targets*, 12.7.2023, *https://digital-strategy.ec.europa.eu/en/library/investment-and-funding-needs-digital-decade-connectivity-targets*

Questa posizione, consegnata in una lettera-appello sottoscritta da ventidue operatori Telco, tra cui Telecom Italia, Vodafone, BT, Orange e Deutsche Telekom[47], si articola intorno a due argomenti principali.

In primo luogo, si parte dalla constatazione che le grandi imprese tecnologiche, benché responsabili di un incremento annuo del traffico annuo di dati tra il 20% e il 30%, contribuiscono ai costi di trasporto dei dati in misura insufficiente a coprire gli investimenti necessari per l'ampliamento delle reti, che usano come l'ultimo miglio per dialogare con i clienti finali. In tale contesto, è paradossale che alcuni fornitori di servizi *cloud* applichino ai propri clienti tariffe ottanta volte superiori a quelle da essi stessi corrisposte per l'utilizzo delle reti delle Telco[48].

In secondo luogo, secondo gli operatori, il presente assetto negoziale non offre alcun incentivo economico a ridurre il traffico dati superfluo. La pandemia ha dimostrato che tale riduzione sarebbe possibile senza compromettere l'esperienza degli utenti. Una regolamentazione basata sul principio del *fair share* favorirebbe un utilizzo più responsabile ed efficiente dei dati, contribuendo quindi anche agli obiettivi europei in materia di consumo energetico e riduzione delle emissioni di CO2.

Inoltre, la dinamica concorrenziale dimostra che le risorse liberabili dalle Telco e dirottabili nell'innovazione tecnologica vengono al momento utilizzate per mantenere l'infrastruttura e per adempiere agli obblighi di conformità imposti dalla regolazione asimmetrica, onere questo, che non grava in misura corrispondente anche sui GK.

---

[47] La lettera è disponibile al seguente indirizzo: *https://connecteurope.org/news/call-fair-share-legislation-europe-must-act-protect-its-digital-future*.

[48] Mentre in origine le reti si basavano su uno scambio simmetrico e gratuito di traffico tra molti operatori (*settlement-free peering*), l'attuale ecosistema digitale è dominato da pochi grandi *player* che generano oltre due terzi del traffico globale e ne assorbono la maggior parte del valore. Espandendosi nelle infrastrutture di trasporto intermediarie (*middle mile*, come cavi sottomarini e CDN proprietari), questi Giganti riversano enormi volumi di dati sulle reti di accesso (*last mile*) degli operatori, creando un flusso strutturalmente asimmetrico, che scarica i costi di gestione sulle infrastrutture locali senza un'adeguata compensazione economica. Cfr., VODAFONE, *Report - A Framework for Responsible Use of Networks*, 28.2.2025, p. 18 *https://www.vodafone.com/news/public-policy/responsible-use-of-networks.*

Queste sono le stesse cause identificate da Vodafone nel suo report "A Framework for Responsible Use of Networks" alla base della c.d. "tragedia dei beni comuni": termine preso in prestito dall'economia per indicare quando il consumo eccessivo di una risorsa comune e limitata – qui le reti di telecomunicazioni – è causa del suo esaurimento[49]. Una più equilibrata ripartizione degli oneri di natura regolatoria e finanziaria tra gli operatori del mercato è stata fatta sollecitata a più riprese anche dal Presidente Mario Draghi, che nel suo ultimo Rapporto ha suggerito di estendere ai GK il principio di condivisione dei costi[50]. Del resto, questa equiparazione Telco e GK appare inevitabile conseguenza della futura convergenza dei media; ma i corposi rapporti dell'*Office of Communications* (Ofcom) – l'Autorità Garante per le Comunicazioni del Regno Unito – non seguono questo indirizzo, soprattutto sul terreno del coordinamento delle reti[51], anche se per ragioni squisitamente geopolitiche. Infatti, l'Ofcom ha preferito appiattirsi sulla politica deregolatoria americana piuttosto che difendere la sua posizione di regolatore neutrale per vincere l'isolamento nel quale l'Europa lo aveva relegato.

## 4. *Quale (de)regolazione?*

Ancora un elemento gioca a favore dei GK e quindi a danno delle Telco: i primi operano su un mercato unico e dilatato nel volume di affari; i secondi su una pluralità di piccoli mercati.

---

[49] Alle cause già descritte nel testo – i grandi fornitori di contenuti trattano la rete come gratuita e illimitata e non partecipano ai costanti investimenti per mantenere la rete – Vodafone ne aggiunge una terza: le politiche europee, in particolare l'applicazione rigidamente prescrittiva delle regole sulla neutralità della rete (*Open Internet*), limitano direttamente la capacità degli operatori di gestire l'impatto del traffico e di ridurre le inefficienze sulle loro reti; si veda in proposito: VODAFONE, *Report*, cit., p. 16-28.

[50] M. DRAGHI, *Il futuro della competitività europea*, *Parte B - Analisi approfondita e raccomandazioni*, cit., pp. 79-80: "In particolare, si raccomanda di: […] Incoraggiare la definizione di accordi contrattuali commerciali per la cessazione del traffico dati e la condivisione dei costi dell'infrastruttura tra i fornitori di servizi Internet o gli operatori di telecomunicazioni che possiedono l'infrastruttura e le piattaforme online molto grandi (VLOP) che la utilizzano. Dovrebbe essere prevista la salvaguardia di arbitrati con offerte finali obbligatorie da parte delle autorità nazionali della concorrenza, in caso di fallimento delle trattative entro un periodo di tempo ragionevole".

[51] Non ci soffermeremo oltre su questo aspetto, perché già oggetto di sapiente approfondimento nel contributo di F. ABBONDANTE in questo *Volume*.

Inizialmente[52] si era avviato un processo regolatorio di tipo governo-centrico, che semplificava concentrando nelle mani della Commissione[53] il momento creativo delle regole come quello attuativo. Le Direttive del 2002 prevedevano rimedi, in astratto delineati unitari, ma in concreto affidati per l'individuazione alle ANR, che, entro un ventaglio di correttivi formulati nelle Direttive, avrebbero scelto la misura più appropriata alle specificità del *defeat* da curare, proporzionata, giustificata e compatibile con gli incentivi alla sua esecuzione (art. 8, Dir. Accesso). La prassi prese però la direzione opposta a quella prevista nel Pacchetto: le ANR, nell'esercizio della propria discrezionalità, dettarono discipline diverse le une dalle altre, avviando una gara al rialzo regolatorio (il c.d. *gold-plating*). Ciascuno Stato infatti aggravò il quadro normativo rispetto a quanto previsto nel pacchetto europeo, inserendo nel proprio ordinamento requisiti, obblighi o standard ulteriori[54] rispetto a quelli unitari.

Le imprese di telecomunicazioni, appesantite da questo fardello normativo, si sono rivelate dei concorrenti 'nani' nel confronto con i 'giganti' di oltre oceano, perché la loro capacità di crescere e di restare competitive è stata di fatto soffocata da un regime regolatorio predatorio. Da qui la necessità di procedere quanto prima a sfoltire il carico normativo con l'avvertenza che questa attività deregolativa dovrà essere tenuta lontana dai tagli assoluti e indiscriminati, perché guidata da un approccio *bottom-up*, quello fondato sull'analisi concreta dei fatti e delle condizioni effettive dei

---

[52] G. De Minico, *Le Direttive CE sulle comunicazioni elettroniche dal 2002 alla revisione del 2006. Un punto fermo?*, in P. Costanzo, G. De Minico, R. Zaccaria (a cura di), *I "tre codici" della società dell'informazione*, Torino, 2006, p. 169 ss.

[53] Ivi, p. 186: "Il radicale cambiamento che il pacchetto direttive 2002 sembrava annunciare" non si sarebbe avverato a causa di questa "sequenza di eventi: direttiva-quadro, Raccomandazione e atti vari di soft law, concorrenti tutti a blindare il tessuto normativo non diversamente da quanto era accaduto in precedenza".

[54] M. Draghi, *Il futuro della competitività europea*, *Parte B - Analisi approfondita e raccomandazioni*, cit., p. 369: "La cosiddetta super-equivalenza si verifica quando l'attuazione nazionale di una direttiva va oltre il minimo necessario per conformarsi ad essa. Ad esempio, gli Stati membri possono eliminare le deroghe o le estensioni presenti nell'atto originale; mantenere standard nazionali più severi o più elevati; applicare la direttiva prima del termine stabilito; o recepire con un campo di applicazione più ampio rispetto alla direttiva UE". Cfr. K. Mickute, H*ow to identify and avoid gold-plating EU regulations*, 2020.

mercati, per giungere a eliminare selettivamente le disposizioni superflue dei contesti caratterizzati da un elevato grado di concorrenza, e, di converso, di conservare solo quelle rivelatesi *reasonable*.

Consideriamo l'esempio Italia, dove la TIM, a seguito della cessione della sua rete alla società Fibercop[55], ha contestato la soggezione agli obblighi regolamentari previsti in qualità di operatore verticalmente integrato. Pertanto, la società ha richiesto all'Autorità per le Garanzie nelle Comunicazioni (AGCOM)[56] di valutare la sopravvenuta inapplicabilità dell'obbligo di replicabilità delle offerte al dettaglio di accesso alla rete fissa o, in subordine, di adottare un provvedimento cautelare di immediata sospensione dello stesso dovere[57]. In considerazione della richiesta di TIM e della separazione strutturale della rete, l'Autorità ha avviato un procedimento di ana-

[55] FiberCop è la società alla quale è stata conferita la rete fissa primaria in precedenza detenuta da TIM. Essa nasce da un'operazione di concentrazione – approvata dalla Commissione europea il 30 maggio 2024 – che ha riguardato sia l'infrastruttura di rete primaria di TIM sia la partecipazione di maggioranza da essa detenuta in FiberCop S.p.A., proprietaria della rete secondaria. L'entità risultante dall'operazione, controllata indirettamente dal fondo statunitense KKR, è stata successivamente rinominata "FiberCop".

[56] TIM, con lettera pervenuta il 2 luglio 2024 (Prot. AGCOM n. 182344), ha dichiarato che, in data 1° luglio 2024, le parti hanno dato esecuzione all'operazione precedentemente approvata dalla Commissione europea e che, dunque, TIM ha trasferito il ramo d'azienda alla controparte, sicché essa non è più titolare di rete fissa e cessa di essere un operatore verticalmente integrato. Con successiva lettera (Prot. AGCOM n. 182355), TIM ha affermato di non ritenersi più vincolata agli obblighi regolamentari precedentemente imposti in quanto operatore verticalmente integrato, essendo ora presente sul mercato della rete fissa esclusivamente in qualità di operatore *retail*, alla pari degli altri concorrenti. Infine, con lettera del 2 settembre 2024 (Prot. AGCOM n. 227291), TIM ha ribadito all'Autorità la necessità di accertare la sopravvenuta inapplicabilità, a partire dalla data del *closing* dell'operazione, dell'obbligo di replicabilità delle offerte al dettaglio di accesso alla rete fissa, non essendo più operatore verticalmente integrato. Inoltre, essa ha richiesto l'adozione di un provvedimento cautelare di immediata sospensione di tale obbligo ai sensi dell'articolo 33, comma 8, del Codice, non essendo "in dubbio la sussistenza di circostanze straordinarie, che richiedano ad AGCOM un intervento di urgenza a salvaguardia della concorrenza e, in definitiva, a tutela degli interessi generali degli utenti".

[57] Tale obbligo, noto come "test di replicabilità", consiste nella preventiva comunicazione all'Autorità delle offerte *retail* di TIM con un anticipo di venti giorni rispetto al lancio commerciale, al fine di verificare la replicabilità economica e tecnica delle offerte da parte di un operatore efficiente che utilizzi i servizi *wholesale* (c.d. "other licensed operator", OLA).

lisi dei mercati dei servizi di accesso alla rete fissa[58], finalizzato a verificare i mutamenti di mercato e la possibile persistenza degli obblighi imposti.

Nella fase preliminare, l'AGCOM ha condiviso la ricostruzione di TIM e ha pertanto disposto la sospensione degli obblighi di replicabilità[59], evidenziando come la loro applicazione, in attesa della conclusione dell'analisi di mercato, avrebbe determinato una sproporzionata condizione di svantaggio concorrenziale per la Telco, ora attiva unicamente nel mercato *retail*[60].

La vicenda solleva ulteriori dubbi[61] e presenta profili complessi.

In concomitanza con lo scorporo della rete, TIM ha stipulato con FiberCop un accordo, denominato *Master Service Agreement* (MSA), in base al quale FiberCop si impegna a fornire a TIM, in via esclusiva, i servizi di accesso all'ingrosso, sia passivi che attivi, per quindici anni, con rinnovo automatico per ulteriori quindici anni. Di conseguenza, TIM, da precedente proprietaria della rete, assume ora il ruolo di concessionaria e beneficerà di una posizione di chiaro vantaggio competitivo, potendo accedere alla propria *ex* rete a condizioni economiche agevolate.

---

[58] Cfr. delibera dell'AGCOM n. 315/24/CONS dell'11 settembre 2024, disponibile al *link https://www.agcom.it/sites/default/files/provvedimenti/delibera/2024/Delibera%20315-24-CONS.pdf*.

[59] Cfr. delibera dell'AGCOM n. 406/24/CONS del 23 ottobre 2024, disponibile al *link https://www.agcom.it/sites/default/files/provvedimenti/delibera/2024/406-24-CONS.pdf*.

[60] La decisione dell'Autorità è stata oggetto di ricorso promosso da Open Fiber S.p.A. davanti al TAR Lazio, Sez. IV, che si è pronunciato con la sentenza del 18 aprile 2025, n. 7745. Open Fiber – diretto *competitor* di FiberCop – contestava la sospensione del test di replicabilità, sostenendo che l'AGCOM avrebbe dovuto verificare preliminarmente i contenuti del *Master Service Agreement* tra TIM e FiberCop (*sub infra*) e attendere l'esito dell'analisi di mercato prima di sospendere l'obbligo. Il TAR ha rigettato il ricorso, ritenendo infondate le doglianze, e ha confermato che il test di replicabilità si applica solo agli operatori verticalmente integrati dotati di SPM, al fine di prevenire discriminazioni tra servizi *wholesale* e *retail* e tutelare la concorrenza.

[61] Sorgono però alcuni profili da chiarire: con la cessione della rete da parte di TIM, occorre definire quali obblighi di accesso possano ancora ricadere sull'ex *incumbent* e quale regime regolamentare risulti applicabile a FiberCop, che detiene la rete e opera solo all'ingrosso senza attività a valle. Sul punto, ci asteniamo da ulteriori approfondimenti, perché il tema è già oggetto di ampia trattazione nel contributo di S. Serafini in questo *Volume*.

Su questo profilo sta indagando l'Autorità Garante della Concorrenza e del Mercato (AGCM) al fine di accertare l'eventuale inosservanza dell'articolo 101 TFUE[62]. L'istruttoria AGCM ha individuato, in via preliminare, due profili critici.

Il primo riguarda la durata dell'esclusiva dell'accordo, che si estenderebbe *de facto* per trent'anni: un tempo eccessivo, che limita le opportunità competitive dei rispettivi concorrenti.

Il secondo fattore di preoccupazione riguarda i meccanismi di c.d. "sconti a volume", sconti cioè che scattano raggiunta una certa soglia di traffico: formalmente accessibili a tutti gli operatori senza discriminazioni, essi risulterebbero concretamente raggiungibili esclusivamente da TIM. Ciò potrebbe determinare un vantaggio competitivo ingiustificato a favore di TIM e una possibile cristallizzazione del mercato, ostacolando nuovi ingressi e la crescita di operatori di minori dimensioni.

Ci si chiede, pertanto, se sia compatibile con i principi di tutela della concorrenza escludere ogni forma di regolazione all'ingrosso, pur in presenza di un persistente vantaggio competitivo di TIM. A nostro avviso, l'obbligo di garantire la replicabilità delle condizioni tariffarie andrebbe mantenuto; in caso contrario, si rischierebbe di eliminare integralmente la regolazione senza considerare che una piena concorrenza non sia stata ancora realizzata.

Dunque, l'esempio illustrato ci suggerisce che un alleggerimento normativo non dovrebbe essere condotto in termini generalizzati, bensì modulato *case by case* e in funzione delle specifiche caratteristiche del mercato e dell'area geografica di riferimento.

Al fine di semplificare l'attuale "selva normativa" risulta, dunque, essenziale garantire il giusto equilibrio tra l'anticipazione delle

---

[62] Cfr. provvedimento dell'AGCM n. 31415 di avvio dell'istruttoria 1874 - MASTER SERVICE AGREEMENT TIM-FIBERCOP, ai sensi dell'articolo 14 della legge n. 287/1990, nei confronti di FiberCop S.p.A. e TIM S.p.A. per accertare l'esistenza di violazioni dell'articolo 101 TFUE. L'avvio del procedimento, con termine previsto per il 31 gennaio 2026, segue l'autorizzazione incondizionata alla concentrazione da parte del *Directorate-General for Competition* della Commissione europea del 29 maggio 2024 (Caso n. COMP/M.11386 - KKR / NETCO), che aveva escluso dal proprio esame l'MSA, demandandone la valutazione all'Autorità nazionale. L'operazione era stata autorizzata dalla Commissione Europea.

soglie dell'antigiuridicità e l'indispensabilità delle normative, affinché non si comprometta il principio di innovazione, indispensabile per una competizione equa e dinamica. Per conseguire tale equilibrio, il Rapporto Draghi propone alcune misure concrete[63], che riteniamo di condividere nella loro sostanza.

Una strategia efficace di miglioramento della legislazione a livello unionale dovrebbe fondarsi, innanzitutto, sull'adozione di una metodologia unitaria per la valutazione di impatto normativo. Tale standardizzazione consentirebbe di assicurare coerenza, trasparenza e comparabilità tra i diversi ordinamenti nazionali.

In parallelo, sarebbe opportuno introdurre uno specifico *stress test* normativo mirato alle piccole e medie imprese (PMI), su cui gli oneri legali pesano maggiormente. Un simile strumento permetterebbe di calibrare l'impatto degli interventi legislativi sui soggetti economicamente più vulnerabili.

Si dovrebbe poi procedere all'eliminazione delle norme incoerenti, sovrabbondanti, obsolete e contraddittorie, così da evitare l'incertezza interpretativa e la coerenza complessiva dell'ordinamento.

Parallelamente, la regolazione dovrebbe diventare più agile grazie all'uso sistematico di strumenti di flessibilità – come le clausole di sperimentazione, le clausole di decadenza negli atti legislativi e la cooperazione rafforzata – "al fine di per garantire l'agilità necessaria a tenere il passo con i rapidi progressi tecnologici"[64]. Infine, sarebbe fondamentale ridurre l'eccesso regolatorio derivante dal fenomeno del *gold plating* – precedentemente citato – e limitare l'applicazione rigorosa del principio della *lex specialis*, sì da prevenire sovrapposizioni e conflitti tra disposizioni, garantendo una maggiore coerenza sistemica.

## 5. *L'attenzione al futuro*

La delicatezza della situazione in corso è alla base della decisione della Commissione Europea di introdurre il *Digital Networks*

[63] M. Draghi, *Il futuro della competitività europea*, *Parte B - Analisi approfondita e raccomandazioni*, cit., p. 352.

[64] Ivi, p. 355.

*Act* (DNA)[65] in luogo dello *European Electronic Communications Code*[66].

Una premessa è necessaria: in questo lavoro ci stiamo basando, non su un atto definitivo, ma sul *Briefing* dello *European Parliamentary Research Service* perché la bozza, inizialmente prevista per fine 2025, è stata posticipata per le perplessità espresse dagli operatori[67]. Ebbene, il *Briefing* mira a potenziare l'ecosistema di connettività digitale UE con cinque azioni fondamentali[68], oggetto di posizioni controverse espresse rispettivamente dal Parlamento, Stati membri, Accademia e *stakeholder*[69], trattasi di azioni in parte già anticipate nei Rapporti Letta e Draghi[70].

Leggiamo insieme i cinque punti focali.

Riguardo alla dismissione del rame, l'atto propone un termine per il completamento del passaggio alla fibra: l'80% degli utenti entro il 2028 e la totalità entro il 2030. Molti *stakeholder* ritengono impraticabile una data unica a livello europeo, suggerendo che essa invece debba riflettere il grado di sviluppo infrastrutturale dei singoli Stati membri[71] e, pertanto, essere variabile.

---

[65] All'inizio del 2024, la Commissione ha avviato il dibattito strategico sulle infrastrutture digitali europee con il *White paper* "How to master Europe's digital infrastructure needs?", seguito, il 6 giugno 2025, da una "Call for evidence" che ha raccolto numerosissimi contributi da imprese, autorità nazionali, associazioni e società civile.

[66] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, in *https://eur-lex.europa.eu/eli/dir/2018/1972/oj/eng*.

[67] P. Licata, *Digital Networks Act, rinvio al 2026: ecco tutte le controversie che hanno bloccato la nuova legge sulle Tlc*, in *corrierecomunicazioni.it*, 6.11.2025, *https://www.corrierecomunicazioni.it/telco/digital-networks-act-rinvio-al-2026-ecco-tutte-le-controversie-che-hanno-bloccato-la-nuova-legge-sulle-tlc/*.

[68] European Parliamentary Research Service, *Briefing* , cit., pp. 2-3. Per le reazioni di: ivi, pp. 4-6.

[69] Ivi, pp. 4-6.

[70] "Virkkunen committed to propose a DNA aligned with these reports, her mission letter and stakeholder positions". European Parliamentary Research Service, *Briefing - Digital Networks Act*, maggio 2025, p. 2, in *https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/772864/EPRS_BRI(2025)772864_EN.pdf*.

[71] Secondo il CEP (*Centre for European Policy Network*), la data specificata per la dismissione finale delle reti in rame – 2030 – ha le caratteristiche di un'economia pianificata. Sono gli stessi operatori di mercato che dovrebbero decidere se e quando

Sul fronte dell'armonizzazione dello spettro, la Commissione sostiene la necessità di un regime autorizzatorio comune a livello UE, criticando le attuali disparità tra Stati membri nelle aste e nella durata minima delle licenze; il CERRE (*Centre on Regulation in Europe*) propone invece di prolungare gratuitamente le licenze esistenti introducendo una clausola *use it or lose it*, tale da costringere gli operatori a restituire lo spettro inutilizzato.

Mentre in materia di sicurezza delle reti 5G, la Commissione mantiene una linea rigida contro i fornitori considerati ad alto rischio, quali Huawei e ZTE, a differenza di diversi *stakeholder*, che adottano un'impostazione più pragmatica, basata su test tecnici nazionali e sull'introduzione di uno schema di certificazione europeo obbligatorio; qui sono evidenti le preoccupazioni per la sicurezza nazionale che giustificano la posizione di netta chiusura della Commissione.

Quanto alla protezione dei cavi sottomarini, il *Briefing* prevede iniziative per una *governance* congiunta dell'infrastruttura, inclusa una *toolbox* per la sicurezza e la creazione di una riserva di navi cablate per le riparazioni.

L'ultimo suggerimento riguarda il *fair share*, rispetto al quale l'UE sembra preferire a un finanziamento diretto dei GK meccanismi di risoluzione delle dispute per restituire potere negoziale alle Telco; o in alternativa sceglierebbe anche contributi sociali più ampi, quelli legati all'impatto ambientale[72]. I grandi generatori di

---

ciò avverrà. Non si ritiene una posizione condivisibile: ciò sottende una concezione esclusivamente proprietaria delle reti TLC, che, anche in dominio del singolo, sono beni a rilevanza pubblica e quindi attratti almeno in parte a un regime pubblicistico. Cfr. P. ECKHARDT, *cepPolicyBrief No. 6/2024: Digital Networks Act*, 25.6.2024, p. 2, in *https://www.cep.eu/eu-topics/details/digital-networks-act.html.*

[72] Questa la proposta della Presidente dell'Autorità Garante per le Telecomunicazioni francese Laure de la Raudière, che "submitted the idea to "encourage accountability of Big Tech on their environmental impact. Explaining that end nodes account for 80% of the environmental impact of digital, she pointed out that Big Tech should be held accountable for pushing citizens to use metaverse applications of very high-definition movies, which encourage people to renew their endpoints, leading to a more significant environmental impact". OPEN FUTURE, F*air Share? Tax Big Tech to address environmental sustainability of digital networks instead!*, in *openfuture.eu*, 5.2.2024, *https://openfuture.eu/note/fair-share-tax-big-tech-to-address-environmental-sustainability-of-digital-networks-instead/.*

traffico continuano a opporsi a qualunque forma di *fair share*, sostenendo che tali oneri siano già ricompresi nelle relazioni contrattuali di *transit and peering*.

In sintesi, da questi punti emerge che agli eccessi di regole, di operatori e di mercati la Commissione intende reagire riconducendo la pluralità a unità: un unico mercato delle telecomunicazioni, un'unica disciplina equiordinante Telco-GK e una sola *governance*.

Mentre i primi due punti sono stati già trattati nelle pagine precedenti, qualche riflessione merita ancora la questione dell'unità della *governance*. Come distribuire il potere, diffonderlo tra le ANR o accentrarlo nelle mani della Commissione?

L'alternativa non è cosa di poco conto. Noi propendiamo per la seconda opzione che si mostra sensibile alla nuova fase del rapporto tecnica-mercato-regole[73]. La novità è nel fatto che gli Stati, trovandosi a gareggiare con i grandi continenti, dalla Cina all'America, non si possono permettere di essere presenti sul palcoscenico internazionale con ventisette nani, in queste condizioni rischierebbero di perdere la competizione prima ancora di iniziarla. Ne consegue che anche la prospettiva regolatoria debba assumere una dimensione sovranazionale; dunque, la filosofia macro-competitiva imporrà alla Commissione europea di riappropriarsi dei poteri, inizialmente ceduti alle Autorità nazionali, in proiezione di sviluppare una politica telecomunicativa unitaria e orientata all'obiettivo uguaglianza, da perseguire lungo gli assi verticale e orizzontale. In questo inedito scenario di ecosistema digitale, che corre su coordinate sovranazionali, la tecnica diventa l'immancabile opportunità del nuovo millennio, purché sia usata a beneficio di tutti, imprenditori e cittadini. Diversamente, cioè se impiegata a vantaggio esclusivo di una ristretta cerchia di operatori, cioè se incrementa il potere di chi

[73] Ci sia consentito il rinvio al nostro recente lavoro, dove l'intreccio tecnica e mercato è oggetto di riflessione, *Unione europea - Mercato -Tecnica, Relazione* svolta al 40° Convegno annuale dell'Associazione Italiana dei Costituzionalisti, *L'Unione europea a confronto con la Costituzione della Repubblica italiana*, 10-11 ottobre 2025, Università degli Studi di Torino, ora pubblicato nel sito *AIC*, *https://www.associazionedeicostituzionalisti.it/images/convegniAnnualiAIC/2025_Torino/Giovanna_De_Minico.pdf.*

è già potente, è un moltiplicatore accelerato delle disuguaglianze esistenti. In questo caso, la tecnica dietro un'apparente obiettività e neutralità avrà messo a tacere la vocazione di leva riduttiva delle ingiustizie.

Questa riduzione è un sogno o un concreto impegno che ciascuno di Noi vuole assumersi?

MARCO OROFINO

# LA TUTELA DEI DATI PERSONALI NELLE COMUNICAZIONI ELETTRONICHE: DALLA DIRETTIVA *E-PRIVACY* ALLA CRISI DEL MODELLO *E-PRIVACY*



## 1. *Introduzione*

La tutela dei dati personali e della vita privata nel settore delle comunicazioni elettroniche costituisce ormai da tempo un ambito particolarmente delicato nel quale interagiscono norme costituzionali nazionali dedicate alla tutela della riservatezza, disposizioni della Convenzione europea dei diritti dell'uomo, fonti primarie e atti di diritto derivato dell'Unione europea nonché discipline nazionali.

Sul piano interno, il diritto alla riservatezza non è esplicitamente menzionato come fattispecie autonoma in Costituzione, ma trova fondamento nelle norme costituzionali che tutelano la dignità della persona e la libertà individuale. Esso è tratto in via interpretativa ed estensiva da una lettura congiunta degli articoli 2, 3, 13, 14, 15 e 21 della Costituzione[1].

[1] La Corte costituzionale, a partire dalla sentenza n. 34 del 1973, ha affermato

Sul piano sovranazionale, nella Convenzione europea dei diritti dell'uomo (CEDU), come pure nella Carta dei diritti fondamentali dell'Unione Europea, la tutela della vita privata trova, invece, un riconoscimento espresso e autonomo: l'art. 8 CEDU garantisce il diritto al rispetto della vita privata e familiare[2], mentre gli articoli 7 e 8 della Carta garantiscono, rispettivamente la riservatezza e il diritto fondamentale alla protezione dei dati personali.

Tale intreccio di fonti – costituzionali, convenzionali e unionali – e, a cascata, la sovrapposizione di livelli normativi e istituzionali

---

che "la libertà e la segretezza della corrispondenza e di ogni altro mezzo di comunicazione costituiscono un diritto dell'individuo rientrante tra i valori supremi costituzionali (v., anche, sent. n. 366 del 1991) e che tale libertà ha una stretta attinenza al nucleo essenziale dei valori della personalità nel senso che è "parte necessaria di quello spazio vitale che circonda la persona e senza il quale questa non può esistere e svilupparsi in armonia con i postulati della dignità umana" (v. sentt. nn. 366 del 1991 e 10 del 1993). Da questo discende secondo la Corte un particolare vincolo interpretativo, diretto a conferire a quella libertà, per quanto possibile, un significato espansivo. Questo vincolo ad un'interpretazione espansiva comporta che vada riconosciuto il diritto alla riservatezza dei dati personali, quale manifestazione del diritto fondamentale all'intangibilità della sfera privata (sentenza n. 366 del 1991), così come il diritto di mantenere segreti tanto i dati che possano portare all'identificazione dei soggetti della conversazione, quanto quelli relativi al tempo e al luogo dell'intercorsa comunicazione (sentt. nn. 81 del 1993 e 372 del 2006, 20 del 2019 e 170 del 2023). Questa particolare *vis* espansiva trova un limite solo nel necessario bilanciamento tra la libertà individuale e l'interesse connesso all'esigenza di prevenire e reprimere i reati, vale a dire ad un bene anch'esso oggetto di protezione costituzionale (v. sentt. n. 34 del 1973 e, recentemente, n. 2 del 2023).

[2] La Corte di Strasburgo ha osservato che il concetto di "vita privata" è un termine ampio, non suscettibile di una definizione esaustiva ma che certamente si estende alla protezione dei dati personali riguardanti le informazioni relative alla salute di una persona (si veda Corte EDU, 25 febbraio 1997, *Z c. Finlandia*, n. 22009/93, § 71, Raccolta 1997-I), aspetti dell'identità fisica e sociale dell'individuo (Corte EDU, 7 febbraio 2002, *Mikulić c. Croazia*, n. 53176/99, § 53, CEDU 2002-I), l'identificazione di genere, il nome, l'orientamento sessuale e la vita sessuale (Corte EDU, 6 febbraio 2001, *Bensaid c. Regno Unito*, n. 44599/98, § 47, CEDU 2001-I; Corte EDU, 28 gennaio 2003, *Peck c. Regno Unito*, n. 44647/98, § 57, CEDU 2003-I). Molto importante è in questo senso Corte EDU (Grande Camera), 4 dicembre 2008, *S. and Marper c. Regno Unito*, nn. 30562/04 e 30566/04, in cui la Corte ha stabilito che la conservazione generalizzata e indiscriminata di dati di DNA e di impronte digitali viola l'art. 8 della CEDU. Il riferimento alle nuove tecnologie e ai dati da queste prodotte è continuato in tema di SMS (Corte EDU, 17 dicembre 2020, *Saber c. Norvegia*, n. 459/18 nonché Corte EDU, 5 settembre 2017, Grande Camera, *Bărbulescu c. Romania*, n. 61496/08) e di email (Corte EDU, 3 aprile 2007, *Copland c. Regno Unito*, n. 62617/00, CEDU 2007-I).

fanno del settore delle comunicazioni elettroniche un caso emblematico di costituzionalismo multilivello, nel quale si riflette la logica della governance multilivello tipica dell'ordinamento europeo[3].

Alla luce di tale quadro, il presente contributo si propone di analizzare in modo sistematico la normativa in materia di protezione dei dati nel settore delle comunicazioni elettroniche, con particolare riferimento al Regolamento (UE) 2016/679 (GDPR)[4] ed alla direttiva 2002/58/CE (direttiva *e-Privacy*)[5]. Inoltre si darà conto del tentativo di riforma della direttiva stessa nonché di alcune innovazioni apportate da altri atti appartenenti al c.d. decennio digitale europeo che incidono indirettamente sulla tutela della riservatezza e sulla disciplina del trattamento dei dati personali.

L'analisi si articolerà lungo tre direttrici principali.

In primo luogo, verrà ricostruita la genesi e l'ambito di applicazione della direttiva *e-Privacy*. In secondo luogo, si esaminerà il rapporto tra tale direttiva ed il GDPR, approfondendo i principali nodi interpretativi e applicativi. In terzo luogo si prenderanno in considerazioni le ipotesi di riforma della direttiva *e-Privacy* e le ragioni che hanno condotto la Commissione europea, nel 2025, ad abbandonare definitivamente il progetto nonché le conseguenze di tale stallo sulla capacità della normativa europea di far fronte alle nuove sfide tecnologiche e digitali che si prospettano all'orizzonte.

Sotto il profilo metodologico, la trattazione seguirà un approccio sistematico e giurisprudenziale, volto a evidenziare il dialogo tra le fonti e tra le Corti, nonché le implicazioni pratiche derivanti dalla frammentazione normativa e dalla mancata adozione di un quadro regolatorio unitario.

---

[3] Sia consentito sul tema rinviare a M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Giuffrè, Milano, 2008.

[4] 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 e alla libera circolazione di tali dati* (Regolamento generale sulla protezione dei dati - GDPR), in GUUE L 119 del 4.5.2016, p. 1 ss.

[5] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, *relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (direttiva sulla vita privata e le comunicazioni elettroniche), GU L 201 del 31.7.2002, p. 37-47.

## 2. *La genesi ibrida della direttiva 2002/58/CE a cavallo tra il settore della protezione dei dati personali ed il settore delle comunicazioni elettroniche*

La direttiva 2002/58/CE costituisce ancora oggi uno dei principali strumenti normativi di diritto derivato dell'Unione europea in materia di protezione dei dati personali.

In origine, la direttiva *e-Privacy* si collocava a cavallo tra due differenti *framework* normativi: da un lato quello delle comunicazioni elettroniche, disciplinato dal *Framework 2002* e imperniato sulla direttiva quadro 2002/21/CE[6]; dall'altro quello della protezione dei dati, fondato sulla Direttiva 95/46/CE[7].

Questa posizione intermedia tra il diritto delle comunicazioni e il diritto della protezione dei dati le conferiva una natura ibrida, al tempo stesso settoriale e trasversale che, se da un lato rifletteva l'intreccio sempre più stretto tra la regolazione delle reti e dei servizi di comunicazione elettronica e la tutela dei diritti fondamentali connessi al trattamento delle informazioni personali, da un altro lato, conduceva ad una sovrapposizione sostanziale, istituzionale e financo terminologica tra i due ambiti[8].

---

[6] Il *Framework 2002* si componeva di una direttiva quadro – la Direttiva 2002/21/CE (GU L 108 del 24.4.2002, p. 33-50 – e di quattro direttive speciali: la Direttiva accesso 2002/19/CE (GUUE L 108 del 24 aprile 2002, p. 7-20); la Direttiva autorizzazioni 2002/20/CE (GUUE L 108 del 24 aprile 2002, p. 21-32); la Direttiva sul servizio universale 2002/22/CE (GUUE L 108 del 24 aprile 2002, p. 51-77); e la Direttiva *e-Privacy* 2002/58/CE (GUUE L 201 del 31 luglio 2002, p. 37-47). Ad esse si affiancava la Decisione n. 676/2002/CE sullo spettro radio (GUUE L 108 del 24 aprile 2002, p. 1-6). V. per un'analisi dettagliata F. Donati, *L'ordinamento ammnistrativo delle comunicazioni*, Giappichelli, Torino, 2007; G. De Minico, *La sfida europea sulle telecomunicazioni: autori, regole, obiettivi*, in A. Pace, R. Zaccaria, G. De Minico (a cura di), *Mezzi di comunicazione e riservatezza. Ordinamento comunitario e ordinamento interno*, Jovene, Napoli, 2008, p. 153 ss., e, volendo, M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, cit.

[7] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, GU L 281 del 23.11.1995, p. 31-50. Sul rapporto tra la c.d. direttiva madre e la direttiva 2002/58/CE, v. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46/CE al nuovo regolamento europeo*, Giappichelli, Torino, 2016, p. 130 ss.

[8] Questo intreccio si è accentuato, come si evince sin dall'intestazione, con l'approvazione della direttiva 2009/136/CE del 25 novembre 2009 *recante modifica della*

Con l'approvazione della direttiva (UE) 2018/1972, che ha istituito il Codice europeo delle comunicazioni elettroniche, questo intreccio si è parzialmente interrotto[9].

Il Codice ha, infatti, riunito e sostituito le quattro direttive del "pacchetto telecomunicazioni 2002", ma non la direttiva *e-Privacy*. L'art. 125 del Codice ha riconosciuto l'autonomia e la permanente vigenza della direttiva *e-Privacy* specificando come le norme codicistiche lasciano "impregiudicate le disposizioni (della direttiva) relative alla tutela della vita privata e dei dati personali nel settore delle comunicazioni elettroniche".

In precedenza, nel 2016 (ma con piena applicazione a far data da maggio 2018) il Regolamento UE 2016/679 aveva abrogato la direttiva 95/46/CE. La direttiva *e-Privacy* è rimasta in vigore mentre è cambiata la sua normativa generale di riferimento. Il passaggio dalla direttiva 95/46/CE al Regolamento (UE) 2016/679 segna non soltanto un mutamento di contenuti, ma soprattutto un profondo cambiamento nella struttura delle fonti del diritto europeo in materia di protezione dei dati[10].

Con l'abrogazione della direttiva e l'adozione del Regolamento, l'Unione ha infatti scelto di superare il modello basato sul recepimento nazionale, sostituendolo con uno strumento di applicazione

---

*direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori*. Tale normativa, infatti, insieme alla direttiva 2009/140/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009 *recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica*, era parte del *Telecom Package* che ha modificato il *Framework* 2002. Le due normative sono state recepite con il d.lgs. n. 196 del 2003. Cfr. M. Orofino, *Il Telecom Package: luci ed ombre di una riforma molto travagliata*, in *Riv. it. dir. pubbl. com.*, n. 2, 2010, p. 514 ss.

[9] Sull'impatto di tale codificazione v. G. Gardini, *Il codice europeo delle comunicazioni elettroniche e l'impatto delle tecnologie sulla "dimensione di libertà" dei cittadini europei*, in *Studium Iuris*, n. 2, 2022, p. 135 ss.

[10] In proposito cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46/CE al nuovo regolamento europeo*, cit., spec. pp. 150-152.

diretta e uniforme in tutti gli Stati membri. Ne è derivato un rafforzamento dell'immediatezza e dell'omogeneità della tutela, nonché un ridimensionamento del margine di discrezionalità nazionale.

Tale scelta ha però generato un effetto collaterale di natura sistematica: la direttiva 2002/58/CE, rimasta in vigore come disciplina settoriale, si è trovata in una posizione inedita, divenendo *lex specialis* di un atto direttamente applicabile. In altri termini, oggi la relazione tra *e-Privacy* e GDPR non è solo di specialità materiale, ma anche di specialità formale inversa: una direttiva, che continua a richiedere trasposizione e adattamento nazionali, opera come norma speciale rispetto a un regolamento che ha portata generale e immediata.

Questo rovesciamento del rapporto tradizionale tra le fonti europee produce inevitabili tensioni applicative. Le disposizioni di recepimento della direttiva, in quanto fonti nazionali, si trovano a integrare – e talvolta a derogare – una fonte di rango sovraordinato direttamente efficace, con il rischio di compromettere la coerenza e l'uniformità della tutela nell'intero spazio giuridico europeo.

È in questa prospettiva che deve essere letta la funzione di ponte normativo che la direttiva 2002/58/CE avrebbe dovuto svolgere nel periodo di transizione post-GDPR: un atto ormai strutturalmente subordinato quanto alla tecnica legislativa, ma ancora essenziale per colmare le lacune settoriali del Regolamento in materia di comunicazioni elettroniche.

Questa situazione che, nel disegno complessivo della Commissione europea, avrebbe dovuto durare solo il tempo necessario all'approvazione di un nuovo regolamento in materia di *e-Privacy*, perdura tuttora. Il che determina, come si vedrà, sovrapposizioni e zone grigie nell'*enforcement* della normativa, specialmente in ambiti come la sicurezza delle reti, il trattamento dei dati di traffico e l'uso dei cookie e di altre tecnologie di tracciamento.

## 3. *L'ambito di applicazione ed i contenuti della direttiva* e-Privacy

Al fine di collocare correttamente le questioni aperte occorre partire ricordando che la direttiva *e-Privacy* è stata oggetto di due interventi normativi modificativi.

Il primo, piuttosto limitato, con la direttiva 2006/24/CE, c.d. direttiva *data retention*, dichiarata invalida dalla Corte di giustizia con sentenza dell'8 aprile 2014 (cause riunite C-293/12 e C-594/12), che regolamentava la conservazione (compresi i tempi) di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione[11]. Il secondo intervento normativo, piuttosto esteso, è avvenuto con la direttiva 2009/136/CE con l'obiettivo di aggiornarla al nuovo contesto tecnologico e rafforzare la tutela dei diritti degli utenti nel quadro del più ampio pacchetto telecomunicazioni del 2009.

La versione oggi consolidata è costruita attorno a un presupposto fondamentale ossia la necessità di garantire che lo sviluppo delle nuove tecnologie e dei servizi di comunicazione elettronica avvenga nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche, in particolare del diritto alla riservatezza e alla protezione dei dati personali.

Questo è precisato nel par. 1, dell'art. 1, che fonda l'armonizzazione delle disposizioni nazionali sia sull'obiettivo di "assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali (…) con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche" sia sulla necessità "di assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità". Entrambi gli obiettivi sono da intendersi come indipendenti dalla tecnologia utilizzata per la trasmissione delle comunicazioni.

Per quanto riguarda il suo ambito di applicazione, l'art. 3 prevede che la direttiva *e-Privacy* si applichi al trattamento dei dati per-

[11] La direttiva 2006/24/CE introduceva all'articolo 15 della direttiva 2002/58/CE il paragrafo 1-*bis* che chiariva come le limitazioni al principio di riservatezza delle comunicazioni previste nell'art. 15, par. 1, non si applicassero ai dati la cui conservazione era imposta dalla direttiva 2006/24/CE sulla c.d. *data retention*. La clausola è rimasta tuttavia priva di applicazione sostanziale a seguito della dichiarazione di invalidità della direttiva 2006/24/CE da parte della Corte di giustizia. V. anche per gli effetti di tale pronuncia sulla norma italiana di recepimento, F. VECCHIO, *L'ingloriosa fine della Direttiva Data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *www.dirittticomparati.it*, 12 giugno 2014.

sonali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche, comprese le reti di comunicazione pubbliche che supportano i dispositivi di raccolta e di identificazione dei dati.

Per servizi di comunicazione elettronica si intendono i servizi forniti di norma a pagamento, consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche. Ne sono un esempio i tradizionali servizi di telefonia fissa e mobile, comprensivi sia del traffico voce sia dei servizi SMS, così come i servizi di accesso a Internet forniti dai principali operatori commerciali attraverso reti a banda larga o ultra larga (ADSL, fibra ottica) oppure mediante reti mobili 4G e 5G. Possono essere ricompresi in questa categoria anche i servizi di connettività Wi-Fi pubblica offerti in luoghi aperti al pubblico, nonché i servizi di trasporto del segnale radiotelevisivo forniti su reti via cavo o satellitari, sempre nella misura in cui essi non riguardano i contenuti diffusi, ma esclusivamente l'infrastruttura di trasmissione. Allo stesso modo, devono considerarsi servizi accessibili al pubblico anche le attività di trasmissione di dati svolte dagli operatori che forniscono connettività o trasporto del segnale a utenti finali o ad altri operatori, purché tali prestazioni si risolvano nella messa a disposizione del mezzo trasmissivo.

Rimangono, invece, esclusi i servizi che, pur utilizzando reti pubbliche, forniscono principalmente contenuti o applicazioni – come i servizi di streaming, le piattaforme social, i servizi di posta elettronica basati sul web o le applicazioni di messaggistica OTT – poiché in questi casi l'elemento caratterizzante non è la trasmissione del segnale, ma il contenuto o la funzionalità erogata all'utente.

La nozione di reti di comunicazione pubbliche fa, a sua volta, riferimento a reti utilizzate interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico. Si tratta, dunque, delle reti telefoniche fisse e mobili gestite dagli operatori nazionali, delle reti a banda larga e ultra-larga che consentono l'accesso a Internet, nonché delle reti via cavo o satellitari impiegate per la diffusione e il trasporto dei segnali radiotelevisivi. Rientrano in questa categoria anche le reti di trasporto e dorsali in

fibra ottica messe a disposizione degli operatori per l'erogazione di servizi al pubblico, così come le infrastrutture Wi-Fi distribuite in luoghi aperti al pubblico – quali stazioni ferroviarie, aeroporti, biblioteche o piazze – ogniqualvolta esse siano utilizzate per fornire connettività a un numero indeterminato di utenti.

In questa prospettiva, devono considerarsi escluse dalla nozione di rete pubblica di comunicazione elettronica una serie di infrastrutture che, pur impiegate per il trasporto di segnali, non sono destinate all'erogazione di servizi di comunicazione elettronica al pubblico. Si tratta, innanzitutto, delle reti private realizzate per esigenze interne di soggetti pubblici o privati, come le intranet aziendali, le reti domestiche o le reti universitarie chiuse, il cui utilizzo è ristretto a una cerchia determinata di utenti e non è aperto all'accesso generalizzato del pubblico.

A queste si aggiungono le porzioni di rete gestite dai cosiddetti operatori OTT (Over-The-Top), le quali, pur coesistendo fisicamente con le reti pubbliche e spesso interconnesse con esse, non svolgono la funzione di fornire connettività agli utenti finali. Le infrastrutture degli OTT, quali le *Content Delivery Network*, i sistemi di caching distribuiti, i *data center* e le piattaforme *cloud*, hanno una funzione meramente interna al servizio digitale offerto e vengono utilizzate per ottimizzare la distribuzione dei contenuti o delle applicazioni. Esse si configurano quindi come reti non accessibili al pubblico, certamente destinate all'erogazione di servizi della società dell'informazione, ma, secondo la definizione adottata, non sottoposte alle regole della direttiva.

La direttiva è, quindi, ancorata ad una doppia distinzione tra servizi di comunicazione elettronica accessibili al pubblico (servizi di telefonia, ISP, provider di e-mail) e servizi privati (servizi intranet aziendali, servizi di messaggistica interna) e tra rete pubblica di comunicazione elettronica ossia infrastrutture di telecomunicazioni accessibili al pubblico quali reti telefoniche e reti internet e reti private ossia reti interne aziendali o domestiche, non accessibili al pubblico.

Sempre per quanto riguarda l'ambito di applicazione materiale occorre aggiungere che la direttiva *e-Privacy* si applica alle persone fisiche e, almeno in parte, anche alle persone giuridiche. Questo

perché talune norme riguardano gli abbonati ai servizi di comunicazione elettronica che possono evidentemente essere sia individui sia soggetti collettivi (imprese, associazioni, fondazioni etc.).

L'impianto normativo della direttiva *e-Privacy*, così come aggiornato dalla direttiva 2009/136/CE, si fonda oggi in particolare, su tre assi portanti:

*a*) la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico (articolo 5);

*b*) la sicurezza del trattamento con riferimento ai servizi accessibili al pubblico e alle reti pubbliche (articolo 4);

*c*) la regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookie (articoli 6 e 9, nonché articolo 5, paragrafo 3).

A queste tre macroaree si aggiungono gli interventi specifici e puntuali volti a tutelare gli utenti e riguardanti le comunicazioni indesiderate, gli elenchi abbonati e il trasferimento automatico della chiamata.

### 3.1. *Riservatezza delle comunicazioni e tutela dei dati di traffico e di ubicazione*

Il principio cardine della direttiva 2002/58/CE, sancito dall'articolo 5, è il diritto alla riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico.

La norma dispone che gli Stati membri provvedano a garantirlo attraverso la legislazione nazionale. Nel rinviare alle legislazioni nazionali, la norma europea specifica come debba essere vietata qualsiasi forma di intercettazione o sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza il consenso degli utenti interessati. Esula dal divieto solo la memorizzazione tecnica necessaria alla trasmissione della comunicazione. Appare evidente come la norma costituisca oggi una specifica attuazione, per il settore delle comunicazioni elettroniche, del più ampio diritto al rispetto della vita privata e fa-

miliare dall'articolo 8 della CEDU, dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. Un diritto sancito nella Costituzione italiana e in tutte le Costituzioni degli Stati membri, risultando pure ascrivibile alla categoria delle tradizioni costituzionali comuni[12].

La norma lascia inalterato l'equilibrio esistente tra il diritto dei cittadini alla vita privata e la possibilità per gli Stati membri di prendere i provvedimenti di cui all'articolo 15, paragrafo 1, della presente direttiva, necessari per tutelare la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e l'applicazione della legge penale.

Il che significa che, se da un lato la direttiva *e-Privacy* non pregiudica la facoltà degli Stati membri di effettuare intercettazioni legali di comunicazioni elettroniche o di prendere altre misure, se necessario, per ciascuno di tali scopi, da un altro lato chiarisce come ciò debba avvenire conformemente all'art. 15 della direttiva stessa, che richiama in maniera quasi testuale le condizioni per restringere la libertà di comunicazione ai sensi della CEDU[13].

La giurisprudenza della Corte di giustizia dell'Unione europea ha progressivamente delineato una lettura rigorosa e sistematica dell'art. 15, par. 1, della direttiva 2002/58/CE, consolidando un

---

[12] Com'è noto, la Corte costituzionale con la sentenza n. 81 del 1993, nell'ambito di una pronuncia interpretativa di rigetto ha affermato che "la particolare disciplina predisposta dagli artt. 266-271 c.p.p. sulle intercettazioni … si applica soltanto a quelle tecniche che consentono di apprendere … il contenuto di una conversazione o di una comunicazione … e non sono, pertanto, estensibili a differenti forme di intervento nella sfera di riservatezza delle comunicazioni … né ad aspetti diversi da quello attinente al contenuto delle comunicazioni medesime". Pur non applicando gli artt. 266-271 c.p.p. ai dati di traffico in quanto tali, la Corte ha comunque ritenuto che anche tali dati rientrino nell'area di tutela dell'art. 15 Cost., ossia nella protezione della libertà e segretezza delle comunicazioni. In questo modo ha allargato l'ambito del diritto costituzionalmente tutelato in modo tale "da ricomprendere fra i propri oggetti anche i dati esteriori di individuazione di una determinata conversazione telefonica (identità dei soggetti, tempo e luogo della comunicazione stessa)".

[13] Occorre in proposito rammentare che la direttiva non poteva, nel momento in cui venne approvata, riferirsi direttamente alla Carta dei diritti fondamentali dell'UE che era stata proclamata nel contesto del Consiglio europeo di Nizza, il 7 dicembre 2020, ma senza entrare formalmente in vigore. La Carta è divenuta giuridicamente vincolante solo con l'entrata in vigore del Trattato di Lisbona il 1° dicembre 2009.

orientamento fortemente garantista in materia di conservazione e trattamento dei dati relativi alle comunicazioni elettroniche.

Fin dalle sentenze *Digital Rights Ireland* e *Tele2 Sverige*[14], la Corte ha chiarito che la direttiva *e-Privacy* costituisce attuazione diretta degli artt. 7 e 8 della Carta dei diritti fondamentali e che il principio generale di riservatezza delle comunicazioni, sancito dagli artt. 5, 6 e 9 della direttiva, impone agli Stati membri l'obbligo di garantire che comunicazioni e dati ad esse correlati non siano oggetto di archiviazione o trattamento da parte di terzi, salvo che ciò avvenga nel quadro di eccezioni strettamente circoscritte. L'art. 15, par. 1, è pertanto qualificato (*Commissioner of An Garda Síochána*, ptt. 40 e 57)[15]) come disposizione derogatoria, soggetta a interpretazione restrittiva, la cui applicazione non può trasformare l'eccezione in regola, pena lo svuotamento di contenuto del principio di riservatezza.

La Corte ha altresì riconosciuto che qualsiasi misura nazionale (dopo la dichiarazione di invalidità della norma europea) che imponga la conservazione dei dati relativi al traffico o all'ubicazione comporta un'ingerenza nei diritti fondamentali garantiti dagli artt. 7, 8 e 11 della Carta, indipendentemente dall'eventuale sensibilità dei dati o dal concreto uso che ne venga fatto (*Commissioner of An Garda Síochána*, ptt. 44-46 e *La Quadrature du Net*, 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, ptt. 121-123)[16].

L'ingerenza è qualificata come particolarmente grave poiché tali dati sono idonei a rivelare aspetti altamente sensibili della vita privata degli individui, consentendo – anche attraverso trattamenti automatizzati – la ricostruzione dettagliata dei loro spostamenti, delle abitudini di vita, delle frequentazioni e delle relazioni sociali, fino alla formazione di veri e propri profili individuali (*La Quadrature du Net*, ptt. 117-118; *Tele2 Sverige*, ptt. 99-101). Ciò implica che le misure derogatorie devono rispettare il principio dello "stretto necessario", fondarsi su norme chiare, precise e giuridica-

[14] CGUE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Secretary of State for the Home Department*.

[15] CGUE, 5 aprile 2022, causa C-140/20, *Commissioner of An Garda Síochána*, spec. parr. 40 e 57.

[16] CGUE, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e a.*

mente vincolanti e prevedere garanzie procedurali e materiali adeguate contro i rischi di abuso (*Digital Rights Ireland*, ptt. 54-69; *Commissioner of An Garda Síochána*, pt. 54).

Un ulteriore asse centrale della giurisprudenza riguarda la qualificazione degli obiettivi di interesse generale che possono legittimare tali deroghe. La Corte ha affermato che solo finalità di rango particolarmente elevato, come la salvaguardia della sicurezza nazionale, sono idonee a giustificare misure di conservazione generalizzata e indiscriminata dei dati (*La Quadrature du Net*, cit., ptt. 135-139; *Commissioner of An Garda Síochána*, pt. 58), e ciò esclusivamente in presenza di una minaccia grave, reale e attuale o prevedibile, accertata tramite controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente.

Per contro, negli ambiti della prevenzione, ricerca e repressione dei reati, solo la lotta ai reati gravi può giustificare ingerenze significativamente invasive, senza tuttavia consentire – secondo costante giurisprudenza – la conservazione generalizzata e indiscriminata dei dati di traffico e di ubicazione (*Tele2 Sverige*, ptt. 107-112; *La Quadrature du Net*, cit., ptt. 140-144; *Commissioner of An Garda Síochána*, cit., pt. 65; *VD e SR* 20 settembre 2022 C-339/20 e C-397/20[17]).

Al di fuori del perimetro ristretto della sicurezza nazionale, la Corte ammette esclusivamente forme meno intrusive di conservazione dei dati. Tra queste rientrano: la conservazione mirata, delimitata secondo criteri oggettivi e non discriminatori relativi alle categorie di persone interessate o al contesto geografico (*La Quadrature du Net*, ptt. 150-152); la conservazione generalizzata e indiscriminata degli indirizzi IP assegnati all'origine della connessione, per un periodo limitato allo stretto necessario (*La Quadrature du Net*, pt. 150); la conservazione generalizzata dei dati identificativi di base degli utenti (*Tele2 Sverige*, cit., pt. 157); e la conservazione rapida ("quick freeze") disposta mediante ordine giudiziario o dell'autorità competente (*La Quadrature du Net*, cit., pt. 159).

Complessivamente, la Corte ha così sviluppato un sistema coerente che, pur riconoscendo obblighi positivi degli Stati nella tutela

[17] CGUE, 20 settembre 2022, cause riunite C-339/20 e C-397/20, *VD* e *SR*.

della sicurezza e nella protezione delle persone vulnerabili, preserva il primato del principio di riservatezza delle comunicazioni e circoscrive con rigore le condizioni che possono giustificare deroghe, confermando una lettura dell'art. 15, par. 1, ancorata a un elevato livello di tutela dei diritti fondamentali.

Un punto assai interessante che emerge tanto dal dato normativo che da quello giurisprudenziale è che la direttiva *e-Privacy* riconosce che la riservatezza delle comunicazioni implica non soltanto la protezione del contenuto della comunicazione, ma anche dei dati relativi al traffico.

Si tratta dei dati che accompagnano la comunicazione e che sono ritenuti anch'essi idonei a rivelare aspetti essenziali della vita privata degli individui potendo infatti consentire un'accurata ricostruzione di relazioni sociali, spostamenti geografici, abitudini di vita, preferenze anche intime dell'utente, e quindi incidere in modo profondo sulla sua sfera personale.

La definizione normativa di tali dati ai sensi della direttiva è piuttosto concisa per cui si tratterebbe di "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione". Questi dati comprendono, ad esempio: l'origine e la destinazione della comunicazione (numeri chiamante e chiamato, indirizzi IP, ecc.); la data, l'ora, la durata e il tipo di comunicazione; l'apparecchiatura utilizzata (es. IMEI, indirizzi MAC); la posizione del dispositivo al momento della comunicazione.

Essi sono nel linguaggio tecnico i c.d. metadati ossia le informazioni che descrivono il flusso delle comunicazioni su una rete, ma non specificamente il contenuto puntuale della medesima.

### 3.2. *Sicurezza delle reti e dei servizi di comunicazione*

Accanto al principio di riservatezza delle comunicazioni, la direttiva 2002/58/CE attribuisce un ruolo centrale al tema della sicurezza dei dati e delle reti.

L'art. 4, par. 1, impone ai fornitori di servizi di comunicazione elettronica accessibili al pubblico l'obbligo di adottare misure tecniche e organizzative adeguate a salvaguardare la sicurezza dei pro-

pri servizi, nel caso congiuntamente con il fornitore della rete pubblica di comunicazione, assicurando un livello di protezione proporzionato al rischio. Un rischio che deve essere parametrato sulla rete e sul servizio utilizzato così come sui dati trattati.

Il par. 1-*bis* identifica le misure minime di sicurezza prevedendo che i fornitori delle reti e dei servizi debbano quanto meno: *a*) garantire che i dati personali siano accessibili solo al personale autorizzato; *b*) tutelare i dati personali archiviati e trasmessi tanto dalla distruzione e dalla alterazione (siano esse accidentali o meno) quanto da archiviazione, trattamento, accesso o divulgazione non autorizzata; *c*) garantire l'attuazione di una politica di sicurezza. Con riferimento a tali misure minime così come ad altre adottate il compito di controllarne il rispetto è posto in capo all'Autorità indipendente competente.

Nell'ottica di garantire una maggiore trasparenza e comprensione dei rischi, i parr. 2 e 3 dell'art. 4 impongono anche al fornitore di un servizio di comunicazione elettronica un doppio obbligo di notifica. Il primo nel caso in cui rilevino un particolare rischio di violazione della sicurezza della rete pubblica. Il secondo nel caso in cui si verifichi effettivamente un *data breach*. In entrambi i casi la notifica deve essere effettuata innanzitutto a favore dell'Autorità competente e solo nei casi più gravi anche a favore degli abbonati o di altra persona coinvolta.

Si tratta di un precedente significativo rispetto al modello generale di notifica dei *data breach* poi previsto dal Regolamento (UE) 2016/679 (articoli 33 e 34). La direttiva *e-Privacy* ha dunque, in questo caso, anticipato, ancorché in ambito settoriale, l'esigenza di garantire trasparenza e tempestività nella gestione degli incidenti di sicurezza, ponendo le basi per un approccio sistemico alla *cybersecurity* come componente della protezione dei dati personali.

La nozione di sicurezza impiegata dalla direttiva assume un significato ampio e multilivello.

Essa include non solo la sicurezza tecnica delle infrastrutture (riservatezza, integrità e disponibilità dei dati), ma anche la prevenzione di accessi non autorizzati, intercettazioni o alterazioni delle comunicazioni, nonché la protezione contro la perdita o la distruzione accidentale dei dati. In questo senso, la sicurezza si configura

come una dimensione funzionale del diritto alla riservatezza, piuttosto che come un ambito autonomo: non si limita a un obbligo tecnologico, ma costituisce un presupposto necessario per l'effettività del diritto fondamentale alla protezione dei dati personali nelle comunicazioni elettroniche.

L'articolo 4 presenta, inoltre, un profilo di governance multilivello, poiché richiede la collaborazione tra i diversi attori del sistema: operatori di rete, fornitori di servizi, autorità di regolazione nazionali e autorità di protezione dei dati. In Italia, ad esempio, la cooperazione tra l'Autorità per le garanzie nelle comunicazioni (AGCOM), il Garante per la protezione dei dati personali e l'Agenzia per la cybersicurezza nazionale (ACN) evidenzia la dimensione interistituzionale della sicurezza dei servizi digitali.

La progressiva convergenza tra protezione dei dati personali e sicurezza informatica si riflette oggi anche nel nuovo quadro europeo: la direttiva *e-Privacy* convive, infatti, con la Direttiva (UE) 2022/2555 (NIS 2), che definisce obblighi di sicurezza e di notifica a carico di un'ampia gamma di soggetti operanti nei settori critici e nei servizi digitali essenziali tra cui specificamente i fornitori di reti pubbliche e i fornitori di servizi di comunicazione elettronica accessibili al pubblico. Tali obblighi si aggiungono a quelli previsti dalla direttiva *e-Privacy*. Questo, pur confermando che la sicurezza delle reti non è più un mero requisito tecnico, ma un elemento strutturale della *governance* europea del rischio digitale, determina una sovrapposizione di obblighi meritevole di attenzione[18].

### 3.3. *La regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookies*

La terza macroarea su cui interviene la direttiva *e-Privacy* è la regolamentazione dell'uso dei dati di traffico, dei dati di ubicazione e dei c.d. cookie.

---

[18] V. per un'analisi complessiva di tali strumenti e per l'emersione di una nuova dimensione della cybersecurity, E. LONGO, *La disciplina della cybersecurity nell'Unione europea e in Italia*, in *La regolazione europea della società digitale*, cit., p. 203 e ss.; M. PIETRANGELO, *La dimensione plurale della cybersicurezza: da potere invisibile a processo collaborativo*, in *Rivista Italiana di Informatica e Diritto*, 2, 2024, p. 13 e ss. La natura

*Per quello che attiene ai dati di traffico*, l'articolo 6 della direttiva *e-Privacy* definisce in modo puntuale le condizioni e i limiti entro i quali i fornitori di reti pubbliche o di servizi di comunicazione elettronica possono, in quanto titolari, trattare i dati degli utenti e/o degli abbonati.

Il par. 1 dell'art. 6, dispone la regola generale per cui essi devono essere cancellati o resi anonimi non appena cessano di essere necessari per garantire la trasmissione della comunicazione. Questa previsione è certamente in linea con il principio di finalità del trattamento inteso in senso stretto.

A questa previsione si accompagnano alcune limitate eccezioni.

La prima eccezione riguarda la possibilità di continuare a trattare i dati necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione. Questo, specifica la norma, è legittimo solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. In ogni caso, comunque, l'abbonato o l'utente devono essere informati sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento per le finalità su esposte.

La seconda eccezione è per i trattamenti connessi alla conservazione dei dati al fine della salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica nonché della prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. In questo caso, dopo che la Corte di giustizia ha dichiarato l'invalidità della direttiva *data retention* sono gli Stati membri a definire i termini di conservazione di tali dati.

La terza eccezione, introdotta nel 2009, riguarda il trattamento dei dati ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto. Il par. 3 dell'art. 6 prevede che il fornitore di un servizio di comuni-

---

di direttiva di tali strumenti implica una loro trasposizione sul piano interno. V. in proposito A. Iannuzzi, *Considerazioni sul disegno di legge «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici» (AC 1717)*, in *Rivista Italiana di Informatica e Diritto*, 1, 2024, p. 59 ss.

cazione elettronica accessibile al pubblico possa trattare i dati nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, alla condizione esclusiva che l'abbonato o l'utente a cui i dati si riferiscono abbiano espresso preliminarmente il proprio consenso. Così come lo hanno prestato, specifica la disposizione, agli abbonati o agli utenti deve essere consentita la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.

Per ognuna delle citate eccezioni, resta inteso che l'attività di trattamento deve essere sempre effettuata da personale specificamente autorizzato, nel rispetto del principio di stretta necessità e delle garanzie di sicurezza e riservatezza previste dal diritto europeo. Inoltre, la normativa riconosce alle autorità competenti la possibilità di accedere ai dati di traffico soltanto nei casi previsti dalla legge, in particolare per la risoluzione di controversie in materia di interconnessione e fatturazione o per esigenze di giustizia e sicurezza pubblica.

*Analogamente, l'articolo 9 disciplina l'uso dei dati di ubicazione* – ossia delle informazioni diverse dai dati di traffico che indicano la posizione geografica degli utenti o degli abbonati di reti e servizi di comunicazione elettronica – quando tali dati non sono strettamente necessari alla trasmissione della comunicazione stessa.

Il par. 1 dell'art. 9 prevede che il loro trattamento, nei limiti e per la durata strettamente necessari alla fornitura di un servizio a valore aggiunto, sia lecito solo se essi siano resi anonimi, fuoriuscendo dunque dal perimetro di applicazione della norma in materia di dati personali, o dietro consenso esplicito e previamente informato dell'utente o dell'abbonato.

Il consenso al trattamento deve essere in ogni momento revocabile sia in via definitiva, come è nella logica, sia, in questo caso, in via provvisoria. In proposito, il par. 2 dell'art. 9 prevede che l'utente e l'abbonato devono avere la possibilità "di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni".

L'impianto complessivo della direttiva riflette quindi un modello di tutela preventiva, fondato sull'idea che la protezione della

riservatezza debba operare non *ex post*, ma al momento stesso della generazione e della trasmissione dei dati.

Infine, *per quanto riguarda la regolazione dei c.d. cookies*, l'articolo 5, paragrafo 3, introduce (dopo la riforma del 2009) una specifica disciplina per l'uso di tecnologie di memorizzazione o di accesso a informazioni nei terminali degli utenti[19].

Fanno eccezione soltanto i casi in cui l'archiviazione o l'accesso ai dati siano "strettamente necessari" per effettuare la trasmissione di una comunicazione o per fornire un servizio esplicitamente richiesto dall'utente (ad esempio, *cookies* tecnici di sessione o di bilanciamento del carico).

La c.d. "cookie rule" prevede che gli Stati membri garantiscano che la memorizzazione di informazioni o l'accesso a informazioni già memorizzate nel terminale di un utente siano consentiti solo a condizione del soddisfacimento di una duplice condizione ovvero che

*a*) l'utente abbia ricevuto informazioni chiare e complete in conformità con la direttiva 95/46/CE (oggi ai sensi del GDPR), e

*b*) abbia espresso il proprio consenso in modo preventivo.

Questa disposizione, apparentemente tecnica, ha assunto nel tempo una portata centrale nel dibattito sulla protezione dei dati online.

La Corte di giustizia dell'Unione europea, nella nota sentenza *Planet49 GmbH* (C-673/17, 2019), ha chiarito che il consenso richiesto dall'articolo 5, paragrafo 3, deve essere libero, specifico, informato e inequivocabile[20]. La Corte ha altresì precisato che il consenso deve essere attivo: non è cioè valido un consenso prestato mediante caselle preselezionate o con formule di *opt-out*; che il consenso deve essere espresso con un'azione positiva inequivocabile (ad esempio, la selezione esplicita di un'opzione); e che la regola si applica indipendentemente dalla natura dei dati memorizzati, anche se non contengono informazioni personali identificabili, poiché, in

[19] I *cookies* sono file che il fornitore di un sito web installa nel computer dell'utente di tale sito e ai quali il fornitore può nuovamente accedere durante una nuova visita del sito da parte dell'utente, per facilitare la navigazione in Internet o transazioni oppure al fine di ottenere informazioni sul comportamento dell'utente.

[20] CGUE, 1° ottobre 2019, causa C-673/17, *Planet49 GmbH.*

questo caso, il semplice accesso al terminale costituisce un'ingerenza nella sfera privata dell'utente. Di qui l'estensione della norma anche ai dati non personali.

Tali principi sono stati ulteriormente sviluppati dal Comitato europeo per la protezione dei dati (EDPB) nelle Linee guida 5/2020 sul consenso e, più recentemente, nelle Linee guida 2/2023 sull'articolo 5, paragrafo 3, della direttiva *e-Privacy*.

Innanzitutto, l'EDPB ha chiarito attraverso i due interventi che la norma non si limita ai soli *cookies* tradizionali bensì a qualsiasi tecnologia di memorizzazione o accesso che consenta di leggere o scrivere dati sul terminale dell'utente, come ad esempio: identificatori anonimi di pubblicità mobile[21], tecniche di browser finger printing, strumenti di tracciamento cross-device, Software Development Kit (SDK) integrati nelle applicazioni mobili[22], tecniche di rilevamento via Wi-Fi o Bluetooth.

In secondo luogo, il Comitato ha offerto una lettura estremamente restrittiva del criterio della necessità tecnica e, dunque delle ipotesi in cui il consenso preventivo ed informato dell'utente non è richiesto. Nello specifico ha affermato che sono "strettamente necessarie" solo quelle tecnologie di memorizzazione e accesso che sono strettamente indispensabili al funzionamento del servizio. Quelle cioè senza le quali il servizio non potrebbe funzionare. Ogni altra tecnologia – anche se utile a fini statistici o per il miglioramento dell'esperienza utente – richiede sempre il consenso preventivo.

In terzo luogo, l'EDPB ha sottolineato come la disciplina del consenso sia strettamente connessa anche ai meccanismi di *design* e di interfaccia. A tal proposito il Comitato, seguendo le sollecitazioni delle autorità nazionali (in particolare la CNIL francese e il Garante

[21] Un advertising ID è un identificatore univoco e anonimizzato dell'utente. Si tratta di una combinazione di lettere e numeri assegnata a un dispositivo, come uno smartphone, un computer o un tablet. I più noti sono al momento gli *Apple's Identifier for Advertisers* (IDFA), i *Google's Advertising Identifier* (GAID) e gli *Amazon Advertising ID*.

[22] Gli SDK (*Software Development Kit*) integrati nelle applicazioni mobili sono insiemi di strumenti, librerie e componenti software forniti da terze parti o dallo stesso sviluppatore della piattaforma che vengono inseriti all'interno di un app per aggiungere funzionalità senza doverle programmare da zero. Essi possono comportare raccolta di dati, tracciamento degli utenti, o influenzare performance e sicurezza dell'app.

italiano[23]) ha ribadito che *cookie wall*, *scrolling* o navigazione implicita non possono costituire forme valide di consenso, in quanto non garantiscono in modo effettivo la libertà di scelta. Inoltre il consenso deve poter essere rifiutato o revocato con la stessa facilità con cui è prestato, e le opzioni devono essere chiare, simmetriche e prive di pressioni o incentivi indebiti.

Da quanto qui ricostruito può dirsi che sotto il profilo sistematico, la "cookie rule" evidenzia in modo emblematico la complessa interazione tra diritto della protezione dei dati ed architettura tecnologica. Essa incarna plasticamente l'idea che la protezione dei dati non si esaurisca in un problema di liceità del trattamento, ma riguardi *hardware*, *middleware* e *software* nella misura in cui governano anche il controllo dell'accesso ai dispositivi e alle informazioni che essi contengono.

In altri termini, l'articolo 5, paragrafo 3, sposta il baricentro della tutela dalla "circolazione dei dati" alla protezione dell'ambiente digitale personale dell'utente, anticipando quella che oggi viene, comunemente, definita una prospettiva di protezione dei dati *by design*.

### 3.4. *Altre questioni di interesse e profili trasversali della direttiva* e-Privacy

Oltre alle tre direttrici fondamentali – riservatezza delle comunicazioni, sicurezza delle reti e dei servizi, e trattamento dei dati di traffico, ubicazione e terminali – la direttiva 2002/58/CE presenta una serie di profili ulteriori di interesse, che ne completano il quadro sistematico. Si tratta di regole relative agli elenchi abbonati, al trasferimento di chiamata, alla fatturazione e alle comunicazioni indesiderate.

Proprio la *disciplina delle comunicazioni indesiderate a fini commerciali* di cui all'art. 13, della direttiva merita una particolare attenzione in quanto rappresenta uno dei primi interventi organici del legislatore europeo di intervenire in materia di marketing di-

[23] V. in proposito le *Linea Guida cookie e altri strumenti di tracciamento* adottate dal Garante per la Protezione dei Dati Personali il 10 giugno 2021, pubblicate sulla G.U. n. 163 del 9 luglio 2021.

retto elettronico. In questo senso, l'intervento normativo europeo realizzato con la direttiva *e-Privacy* costituisce un passaggio fondamentale nel processo di costruzione di un sistema di tutela della riservatezza nelle comunicazioni digitali.

La norma introduce al par. 1, dell'art. 13 il principio generale del consenso preventivo (c.d. *opt-in*), prevedendo che l'uso di strumenti automatizzati di comunicazione – quali ad esempio dispositivi di chiamata senza operatore, telefax o posta elettronica – per finalità promozionali sia consentito esclusivamente nei confronti di quegli utenti o abbonati che abbiano espresso preliminarmente il loro consenso rispetto allo specifico trattamento dei loro dati di contatto.

La previsione del consenso come unica condizione di legittimità è la prova del fatto che il "legislatore" europeo ha inteso riconoscere all'utente un potere effettivo di autodeterminazione rispetto alla ricezione di messaggi pubblicitari.

Accanto alla regola generale dell'*opt-in*, il par. 2 del medesimo articolo introduce una deroga limitata, nota come c.d. *soft spam*, che consente al fornitore di utilizzare l'indirizzo elettronico del cliente, acquisito nel contesto di una precedente vendita o trattativa commerciale, per promuovere prodotti o servizi analoghi, a condizione che l'interessato sia stato informato in modo chiaro e trasparente e che gli sia garantita in ogni momento la possibilità di opporsi gratuitamente al trattamento dei propri dati per tali finalità.

Questa eccezione, di natura strettamente funzionale, risponde all'esigenza di bilanciare la libertà di iniziativa economica con la tutela dei diritti degli utenti, evitando che la disciplina si traduca in un ostacolo sproporzionato per le attività legittime di comunicazione commerciale. Inoltre, il fatto che la disposizione si limiti ai contatti via email risponde all'obiettivo di minimizzare l'intrusione nella vita privata che, invece, si verifica attraverso la ricezione di chiamate o messaggi indesiderati.

Per quanto riguarda i casi non rientranti nel par. 1 – ossia senza l'uso di strumenti automatici – né nel par. 2 riguardante il c.d. soft spam, l'art. 13 della direttiva consente agli Stati membri un margine di discrezionalità per determinare se adottare un regime di *opt-in* (comunicazioni consentite solo previo consenso) oppure di *opt-out* (comunicazioni vietate solo in presenza di un'esplicita opposizione).

Quale che sia l'opzione prescelta, il legislatore nazionale deve assicurare che le comunicazioni indesiderate possano essere rifiutate senza oneri per l'utente e che siano vietate pratiche scorrette, quali la falsificazione dell'identità del mittente o l'invio di messaggi privi di un indirizzo valido per l'esercizio del diritto di opposizione.

Infine, la disposizione europea prevede meccanismi di tutela giurisdizionale e amministrativa, riconoscendo a chiunque abbia subito un pregiudizio – ivi compresi i fornitori di servizi di comunicazione elettronica – il diritto di promuovere un'azione per far cessare o vietare le violazioni della disciplina. In tal modo, l'articolo 13 concretizza, in un settore specifico, il principio di autodeterminazione informativa dell'individuo, anticipando concetti e strumenti di tutela che saranno successivamente formalizzati e ampliati dal Regolamento (UE) 2016/679 (GDPR). La norma assume pertanto un valore paradigmatico nell'evoluzione del diritto europeo delle comunicazioni elettroniche, segnando il passaggio da una logica meramente economico-concorrenziale a una visione centrata sulla protezione dei diritti fondamentali e sulla responsabilizzazione dei titolari del trattamento nell'ambito delle pratiche di marketing digitale.

In conclusione, come si evince dall'analisi delle tre macroaree d'intervento nonché della disciplina sulle c.d. comunicazioni commerciali, la direttiva 2002/58/CE si configura come un atto di diritto derivato ibrido e settoriale, che ha però anticipato molti principi ed istituti poi consolidatisi nel GDPR, ma che oggi risente dei limiti del suo impianto originario e della frammentazione derivante dai diversi recepimenti nazionali. Queste criticità, insieme alla rapida evoluzione tecnologica e al mutato ecosistema digitale, costituiscono le premesse per comprendere le ragioni dei tentativi di riforma e, al tempo stesso, i motivi del loro fallimento, temi che saranno approfonditi nel paragrafo successivo.

## 4. *Il rapporto tra la direttiva* e-Privacy *e il GDPR: specialità e integrazione*

Nel sistema europeo di tutela dei dati personali, la direttiva 2002/58/CE e il Regolamento (UE) 2016/679 intrattengono un rap-

porto di specialità e complementarità funzionale, non di successione.

Gli artt. 94 e 95 del GDPR chiariscono oggi questi rapporti.

In primo luogo, l'art. 94 del GDPR, dopo aver stabilito al primo comma, l'abrogazione della direttiva 95/46/CE a far data dall'applicazione del GDPR, nel secondo comma specifica che i riferimenti ed i rinvii che la direttiva *e-Privacy* fa alla direttiva 95/46/CE si intendono fatti, dopo l'abrogazione di quest'ultima, al GDPR.

In secondo luogo, l'art. 95 GDPR stabilisce che il Regolamento non impone alle persone fisiche e alle persone giuridiche obblighi supplementari nelle materie per le quali sono soggetti a obblighi specifici fissati dalla direttiva 2002/58/CE (e recepiti sul piano nazionale) a patto che le norme eventualmente sovrapponibili siano ispirate dal medesimo fine.

Le due norme del GDPR perseguono tre obiettivi che devono guidare l'interpretazione nei casi in cui si verifica una sovrapposizione di norme.

Il primo obiettivo è evitare una duplicazione di oneri regolamentari[24].

Il secondo obiettivo è confermare che tra le due fonti si applica, nei casi in cui vi sia sovrapposizione di norme adottate per perseguire gli stessi fini, il criterio di specialità: il Regolamento, prendendo il posto della direttiva 95/46/CE è la nuova norma generale, mentre la direttiva *e-Privacy* rimane la norma speciale.

Il terzo obiettivo è quello di rendere manifesto che, se non c'è sovrapposizione né contrasto tra le due normative europee, la direttiva *e-Privacy* può anche integrare il Regolamento.

Non può sfuggire però come il confine tra prevalenza ed integrazione sia sottile, rimesso come è all'individuazione di obiettivi comuni o meno nel caso di sovrapposizioni normative. Inoltre, non si può dimenticare che il rapporto che in precedenza si ribaltava, completamente, sulle fonti di trasposizione interna, ora crea un'interessante asimmetria perché si instaura tra una fonte regolamen-

[24] Si veda il caso degli obblighi di notifica dei *data breaches* che sono disciplinati in entrambi gli atti normativi.

tare europea (il GDPR) e le fonti nazionali di trasposizione della direttiva adottate dagli Stati membri[25].

Proprio al fine di sciogliere le possibili criticità, l'EDPB ha adottato il Parere n. 5 del 2019[26]. Il Comitato nel definire il rapporto tra le due normative ha parlato di precisazione (specialità) ed integrazione.

Le aree di sovrapposizione che occorre specificamente osservare sono ben note. Esse riguardano:

*a*) il trattamento dei dati di comunicazione (traffico, ubicazione, metadati);

*b*) l'uso dei terminali e delle tecnologie di tracciamento (cookie, identificatori pubblicitari, *fingerprinting*);

*c*) le comunicazioni promozionali automatizzate e il marketing diretto.

I casi più noti di precisazione, e quindi di applicazione del criterio di specialità, riguardano le condizioni di legalità del trattamento. In questo caso la *lex generalis* è l'art. 6 del GDPR che individua le basi giuridiche del trattamento dei dati personali, cioè le condizioni che rendono lecito il trattamento. La norma come noto individua accanto al consenso altre cinque basi legali tra cui vi sono l'esecuzione di un contratto, l'obbligo legale, la salvaguardia degli interessi vitali, l'esecuzione di pubblici poteri e il legittimo interesse del titolare purché non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato.

La direttiva *e-Privacy* richiede, invece, *ex* artt. 5, 6 e 9 il consenso esplicito e preliminare dell'interessato per i trattamenti che consistono nell'archiviazione o accesso ai dispositivi degli utenti, per il trattamento dei dati di traffico, per i trattamenti dei dati rela-

---

[25] Come evidenziato dal Garante europeo della protezione dei dati (EDPS), la permanenza di una direttiva come fonte speciale rispetto a un regolamento direttamente applicabile genera una anomalia strutturale. Cfr. *Opinion 6/2017 on the Proposal for a Regulation of Privacy and Electronic Communications (e-Privacy Regulation).*

[26] EDPB, *Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities* (12 March 2019). Cfr. C. Etteldorf, *EDPB on the interplay between the e-Privacy Directive and the GDPR*, in *European Data Protection Law Review (EDPL)*, 2019, vol. 5, n. 2, pp. 224-231.

tivi all'ubicazione. In questi casi, in quanto *lex specialis* la direttiva *e-Privacy*, e gli atti nazionali di recepimento prevalgono sul GDPR. Il che significa che né il fornitore di una rete pubblica né il fornitore di un servizio accessibile al pubblico possono ricorrere al contratto o all'interesse legittimo come base legale del trattamento.

Questo determina un'evidente asimmetria oggi rispetto ad alcuni fornitori di servizi di comunicazione c.d. *overthetop* che offrono servizi di comunicazione ormai ampiamente sostitutivi rispetto quelli forniti dai fornitori di servizi di comunicazione elettronica.

Per quanto riguarda l'integrazione tra le norme del GDPR e quelle della direttiva *e-Privacy* si pensi alle numerose disposizioni di quest'ultima che hanno lo scopo proteggere gli "abbonati" ad un servizio di comunicazione elettronica accessibile al pubblico.

Come noto, l'ambito di applicazione del GDPR riguarda i dati personali delle sole persone fisiche laddove invece la precedente direttiva consentiva agli Stati membri di estendere la protezione alle persone giuridiche.

Gli abbonati a un servizio di comunicazione elettronica accessibile al pubblico possono essere, come la direttiva *e-Privacy* specifica, sia persone fisiche che persone giuridiche. La direttiva *e-Privacy*, integra in questo caso la tutela che il GDPR offre ai diritti fondamentali delle persone fisiche e in particolare il loro diritto alla vita privata, con la tutela degli interessi legittimi delle persone giuridiche.

Lo stesso accade per la c.d. *cookie rule* di cui all'art. 5 della direttiva *e-Privacy*. Le norme ivi contenute si applicano, come precisato dalla Corte di giustizia, anche ai dati che non consentono l'identificazione della persona a cui si riferiscono e che, dunque, ai sensi del GDPR non sono dati personali e, quindi fuoriescono dal perimetro dell'intervento regolamentare.

Vi sono poi casi, come ad esempio, per ciò che riguarda le misure di sicurezza in cui specialità ed integrazione si sovrappongono. Da un lato, la direttiva *e-Privacy* richiede al fornitore di reti o servizi di comunicazione elettronica l'adozione di specifiche misure di sicurezza, secondo una logica che in parte richiama quella della direttiva 95/46/CE e, dall'altro lato, il GDPR impone loro di definire

le misure di sicurezza necessarie sulla base di una valutazione del rischio.

In questo si vede in modo evidente come la direttiva *e-Privacy*, adottata in un contesto tecnologico precedente all'entrata in vigore del Regolamento, continui a disciplinare il trattamento dei dati personali nel settore nelle comunicazioni elettroniche, dentro il modello normativo precedente che pure ha contribuito in alcuni casi a superare.

Un ulteriore profilo critico in cui sono possibili deleterie sovrapposizioni è quello del regime di *enforcement*.

Il GDPR prevede che le Autorità nazionali di controllo (e il Comitato europeo di protezione dei dati) siano i bracci armati del regolamento al fine di garantirne un'attuazione uniforme[27]. Esse, garantite da una posizione di indipendenza, hanno poteri trasversali (cioè su ogni trattamento dati) molto ampi ed incisivi al fine *ex* art. 51, par. 1 di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. Rispetto a questa competenza generale, le limitazioni o le deroghe sono formulate in modo esplicito.

Ad esempio, il Regolamento stesso identifica un'eccezione per i trattamenti di dati personali effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali (articolo 55, paragrafo 3) e una possibilità di derogare a questo mandato per i trattamenti effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria (articolo 85).

La direttiva *e-Privacy* non contiene al suo interno disposizioni analoghe. L'art. 15-*bis*, introdotto nel 2009 e rubricato *Attuazione e controllo dell'attuazione* si limita a specificare che gli Stati membri debbano garantire che l'autorità nazionale competente e, se del caso, altri organismi nazionali dispongano dei poteri per far cessare le violazioni così come delle risorse e delle competenze necessarie. A questa previsione si aggiungono solo una pluralità di rinvii all'autorità nazionale di regolazione, c.d. ANR disciplinata dalla direttiva

[27] Così F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati*. II. *Il Regolamento europeo 2016/679*, Giappichelli, Torino, 2016, p. 103.

quadro 2002/21/CE, come "l'organismo o gli organismi incaricati da uno Stato membro di svolgere le funzioni di regolamentazione fissate dalla presente direttiva e dalle direttive particolari"[28]. La direttiva *e-Privacy* letta alla luce della direttiva 2002/21/CE lasciava dunque agli Stati il compito di ripartire i compiti di sorveglianza tra le Autorità di regolazione nel settore delle comunicazioni elettroniche e le autorità di protezione dei dati. Nella quasi totalità degli Stati membri si è optato per una suddivisione tra diverse Autorità. Il che ha ovviamente generato non poche sovrapposizioni ed incertezze nella *governance* ed ha inciso negativamente sulla coerenza applicativa[29].

Il punto in questione è quindi se, nell'ambito dei rapporti tra GDPR e direttiva *e-Privacy*, sia ancora consentita una deroga alla competenza generale delle autorità per la protezione dei dati nei casi in cui al trattamento in questione si applicano le disposizioni della direttiva *e-Privacy*.

Nel caso italiano, che rappresenta in questo caso una best practice, le funzioni di sorveglianza della direttiva *e-Privacy* sono state tutte affidate al Garante per la protezione dei dati prevedendo al contempo un meccanismo di cooperazione sistematica (tramite un Accordo interistituzionale) tra il Garante e l'Autorità per le garanzie nelle comunicazioni, che è invece stata notificata come Autorità nazionale di regolazione nel settore delle comunicazioni elettroniche.

Come emerge dalle questioni proposte, il rapporto tra la direttiva *e-Privacy* (le discipline nazionali) e il GDPR non può essere descritto unicamente in termini di specialità, ma piuttosto di integrazione reciproca e tensione sistemica. In teoria, la direttiva *e-Privacy* assicura un livello di tutela più elevato per la riservatezza delle comunicazioni, mentre il Regolamento ne garantisce l'armonizzazione

[28] Tra l'altro occorre rilevare che le ANR, a norma della direttiva quadro sono indipendenti nei confronti degli operatori e, di conseguenza, obbligatoriamente nei confronti del Governo solo se lo Stato mantiene il controllo di uno o più operatori di mercato. Il che naturalmente rende il requisito dell'indipendenza diverso rispetto a quanto previsto nel GDPR.

[29] Cfr. J. Dumortier, E. Kosta, *e-Privacy Directive: Assessment of Transposition, Effectiveness and Compatibility with the Proposed Data Protection Regulation*, studio per la Commissione europea, DG CONNECT, 10 giugno 2015.

minima e i principi generali di trattamento. Nella sostanza però, questo determina, come l'EDPB ha sottolineato un "fragmented landscape" che ostacola la prevedibilità per gli operatori economici e riduce l'efficacia delle tutele per gli interessati[30].

## 5. *Il tentativo (non riuscito) di sostituire la direttiva* e-Privacy *con un nuovo regolamento settoriale e la ricerca di una nuova strada*

La mancata armonizzazione dei recepimenti nazionali, unita alla rapida obsolescenza tecnologica, ha reso il quadro normativo instabile e frammentato, ponendo le basi per la proposta di un nuovo Regolamento *e-Privacy*, concepito per sostituire l'attuale direttiva con uno strumento di portata uniforme.

Il GDPR definiva, nel considerando 173, la coesistenza con la direttiva *e-Privacy* come provvisoria prevedendo che essa avrebbe dovuto essere presto aggiornata. D'altra parte già nel 2015, la Commissione europea nel contesto della Strategia per il Mercato unico digitale, aveva preannunciato l'avvio di un processo di revisione della direttiva *e-Privacy* al fine di renderla coerente con il nuovo quadro generale in materia di protezione dei dati personali nonché di superare la differenziazione normativa tra fornitori di servizi di comunicazione elettronica e fornitori di servizi digitali[31].

Nell'ambito del Refit dedicato alla direttiva *e-Privacy*, la Commissione europea ha individuato due criticità principali[32]. La prima è la frammentazione dovuta ai recepimenti nazionali eterogenei, ca-

---

[30] EDPB, *Parere 5/2019*, cit., § 15.

[31] Commissione europea, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final, Bruxelles, 6 maggio 2015.

[32] Il *Regulatory Fitness and Performance Programme* (Refit) è il programma dell'Unione europea per l'adeguatezza e l'efficacia della regolamentazione. Esso, introdotto nel 2012, mira a rendere la legislazione dell'UE più semplice, ridurre gli oneri amministrativi, garantire che la normativa produca risultati concreti. Non si tratta di un atto normativo bensì di un processo permanente di revisione applicato a tutta la produzione normativa dell'UE. Commissione europea, *Programma per l'adeguatezza e l'efficacia della regolamentazione (REFIT). Bilancio della regolamentazione dell'UE*, COM(2012) 746 final, Bruxelles, 12 dicembre 2012.

pace di ostacolare la certezza del diritto e la parità di condizioni nel mercato interno; la seconda è l'inadeguatezza tecnologica della direttiva rispetto ai nuovi servizi digitali e alle piattaforme over-the-top (OTT)[33].

Sulla base delle risultanze del *refit*, la Commissione presentò nel 2017 la proposta di un nuovo regolamento *e-Privacy* che avrebbe dovuto abrogare la direttiva 2002/58/CE ed assicurare uniformità, immediatezza applicativa e coerenza, anche sistematica, con il GDPR[34].

Il regolamento proposto era concepito come un testo di complemento settoriale al GDPR, volto a disciplinare in modo unitario: *a*) la riservatezza delle comunicazioni elettroniche, estesa ai servizi di messaggistica, VoIP, e-mail e social media; *b*) l'uso dei dispositivi terminali e delle tecnologie di tracciamento (cookie, identificatori pubblicitari, IoT); *c*) le comunicazioni a fini di marketing diretto; *d*) le interferenze legittime per motivi di sicurezza pubblica o prevenzione dei reati[35].

Nonostante l'urgenza riconosciuta dalla Commissione europea così come dalle altre Istituzioni europee, il processo legislativo si è arenato sin dalle prime fasi dei negoziati in seno al Consiglio dell'Unione europea.

Diverse ragioni politiche e istituzionali ne hanno determinato lo stallo.

In primo luogo, gli Stati membri hanno espresso posizioni divergenti sulla ripartizione delle competenze tra autorità nazionali: alcuni ritenevano opportuno mantenere un ruolo per le autorità di

---

[33] Commissione europea, *Evaluation and review of the e-Privacy Directive (2002/58/EC)*, SWD(2016) 223 final, Bruxelles, [2016].

[34] *Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla privacy e le comunicazioni elettroniche)*, COM(2017) 10 final, Bruxelles, 10 gennaio 2017. V. in proposito, anche con riferimento agli apporti del Parlamento, durante l'iter E. Gil González, P. De Hert, V. Papakonstantinou, *The Proposed e-Privacy Regulation: The Commission's and the Parliament's Drafts at a Crossroads?*, *Brussels Privacy Hub - Working Paper*, vol. 6, n. 20, marzo 2020, *https://brusselsprivacyhub.eu*.

[35] Cfr. L. Bolognini, C. Bistolfi, G. Crea, *e-Privacy Regulation: legal principles and impacts on the digital economy*, Studio dell'Istituto Italiano per la Privacy e la Valorizzazione dei Dati, 21 marzo 2018, disponibile su *www.istitutoitalianoprivacy.it*.

regolazione delle comunicazioni, mentre altri (tra cui l'Italia) preferivano attribuire la vigilanza esclusiva alle autorità di protezione dei dati personali[36].

In secondo luogo, le imprese del settore digitale hanno esercitato forti pressioni contro la generalizzazione del regime del consenso, a discapito del ricorso all'interesse legittimo, ritenendolo eccessivamente oneroso per i modelli di business fondati sulla pubblicità comportamentale.

Infine, la complessità tecnica del testo e la necessità di coordinarlo con altri strumenti normativi (in particolare la Direttiva NIS 2, il Codice europeo delle comunicazioni elettroniche e, più tardi, il *Digital Services Act*) hanno ulteriormente rallentato i lavori.

Dopo ripetuti tentativi di compromesso e varie versioni di testo su cui non si è mai raggiunto un accordo politico definitivo tra Commissione, Consiglio e Parlamento europeo, l'attenzione delle istituzioni si è progressivamente spostata verso nuove priorità, legate alla transizione digitale e all'economia dei dati, sfociate nell'adozione di numerosi Regolamenti, i c.d. *Acts* con cui l'Unione europea mira a regolare la società digitale europea (*Digital Services Act*, *Digital Markets Act*, *Data Governance Act*, *Data Act*, *AI Act*)[37]. Pur non trattandosi di normative in materia di protezione di dati (e tanto meno volte ad abrogare la direttiva *e-Privacy*), esse hanno in parte assorbito la funzione di aggiornamento tecnologico, affrontando questioni – come la pubblicità personalizzata, la moderazione dei contenuti o l'interoperabilità dei servizi – che incidono indirettamente anche sulla sfera della riservatezza.

---

[36] Sulle divergenze emerse in seno al Consiglio v. i *Progress report on the proposal for a Regulation on Privacy and Electronic Communications*, doc. 9079/18 (25 maggio 2018); ST-14491/18 INIT (25 maggio 2018); ST-12891/20 INIT (18 novembre 2020), dove si dà atto che, mentre alcune delegazioni potevano sostenere l'attribuzione delle competenze alle autorità responsabili dell'applicazione del GDPR, "most delegations seek further flexibility with regards to the supervisory authorities".

[37] Per un'analisi di tali interventi normativi sia consentito rinviare a F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024. V. specificamente sul modello di regolazione europeo e sul ruolo della tecnica, G. De Minico, *Unione europea, mercato, tecnica*. Relazione al Convegno annuale dell'Associazione Italiana dei Costituzionalisti su "L'Unione europea a confronto con la Costituzione della Repubblica italiana" tenutosi a Torino il 10-11 ottobre 2025, in corso di pubblicazione sulla Rivista AIC.

Nel 2025, dopo oltre otto anni di negoziati infruttuosi, la Commissione ha infine deciso di ritirare formalmente la proposta di regolamento *e-Privacy*, riconoscendo l'impossibilità di raggiungere un consenso politico nel Consiglio e l'obsolescenza della proposta alla luce delle norme più recentemente approvate[38].

La decisione segna dunque la fine di un lungo processo di riforma, rimasto incompiuto, che lascia il settore delle comunicazioni elettroniche ancora regolato da una direttiva e da ventisette diverse legislazioni nazionali concepite per un'epoca tecnologica ormai superata.

Proprio mentre maturava la decisione di ritirare la Proposta di regolamento *e-Privacy*, la Commissione europea avanzava una Proposta di Regolamento c.d. *GDPR Omnibus*, volto ad emendare la normativa esistente al fine di operare una semplificazione degli obblighi oggi a carico di piccole e medie imprese[39], una Proposta di Regolamento c.d. *Digital Omnibus* volto a semplificare il quadro regolamentare digitale nonché una consultazione pubblica per la definizione di una proposta di regolamento in materia di reti digitali (c.d. *Digital Networks Act*) che si inserisce in una più ampia strategia di revisione dell'intero ecosistema delle comunicazioni elettroniche.

La proposta di regolamento c.d. *GDPR omnibus*, così come presentata dalla Commissione, non prevede alcuna disposizione volta ad abrogare la direttiva *e-Privacy* né parti di essa. Le misure di alleggerimento degli obblighi normativi introdotte dalla proposta – peraltro circoscritte e rivolte principalmente alle piccole e medie imprese – appaiono destinate ad avere un impatto molto limitato sui fornitori di reti e servizi di comunicazione elettronica, i quali, per dimensioni e struttura, normalmente non rientrano nel perimetro soggettivo delle PMI. Inoltre, il contenuto della proposta, volto

[38] V. Allegati I a V a Commissione europea, *Programma di lavoro della Commissione per il 2025*. COM(2025) 45 final, Strasburgo, 11 febbraio 2025.

[39] European Commission, *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures*, COM(2025) 501 final, Brussels, 21 May 2025, 2025/0130 (COD).

essenzialmente a intervenire su obblighi di registrazione, codici di condotta e meccanismi di certificazione, non incide in modo significativo né sulle norme della direttiva *e-Privacy* né sulle corrispondenti disposizioni nazionali di recepimento.

Per quel che riguarda la Proposta di Regolamento *Digital Omnibus*, esso contiene, invece, misure idonee ad impattare direttamente su alcune norme della Direttiva *e-Privacy*[40]. Innanzitutto, la Proposta in questione mira ad abrogare l'art. 4 della direttiva *e-Privacy* riconducendo integralmente la disciplina della sicurezza nell'ambito del GDPR e della direttiva NIS 2[41]. In secondo luogo, si propone la limitazione dell'ambito di applicazione della c.d. *cookies rule* dettata all'art. 5, par. 3 della direttiva *e-Privacy* che rimane in vigore solo per la memorizzazione e l'accesso ai dispositivi di abbonati e/o utenti che siano persone giuridiche. Per ciò che riguarda, invece, la memorizzazione e l'accesso ai dispositivi di persone fisiche la nuova proposta mira ad integrare una nuova *cookie rule* orizzontale nel GDPR superando, quindi, la specialità relativa alle reti pubbliche e ai servizi accessibili al pubblico di comunicazione elettronica attualmente prevista ai sensi della direttiva *e-Privacy*[42].

Assai rilevante è, inoltre, nella Proposta la nuova definizione di dato personale in cui si specifica come l'identificabilità della persona a cui il dato si riferisce debba essere valutata nel contesto reale e non solo potenzialmente. Questa modifica potrebbe evidentemente incidere anche sulla qualifica di molti dati elettronici come dati personali.

Per quel che attiene all'annunciato *Digital Networks Act*, la proposta di regolamento, inizialmente programmata per il quarto

---

[40] V. *Proposal of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)*, 19 November 2025 {SWD(2025) 836 final}.

[41] Cons. 48 e Art. 5 *Proposal Digital Omnibus.*

[42] V. Cons 44 e art. 3 par. 15 della *Proposal Digital Omnibus* che mira a introdurre nel GDPR l'art. 88a rubricato *Processing of personal data in the terminal equipment of natural persons* al fine di specificare quando è necessario il consenso dell'interessato e quando è possibile prescinderne.

trimestre del 2025 è stata ora posposta a gennaio 2026. Con essa l'Unione europea si propone non soltanto di modernizzare la disciplina delle reti e dei servizi di comunicazione elettronica, ma anche di superare i limiti strutturali derivanti dall'attuale frammentazione del mercato e dalla natura direttiva del Codice europeo delle comunicazioni elettroniche (EECC)[43].

La consultazione preliminare avviata dalla Commissione evidenzia, infatti, come la proliferazione di normative nazionali eterogenee, la lentezza dei recepimenti e l'eterogeneità delle condizioni di autorizzazione e assegnazione dello spettro radio costituiscano oggi uno dei principali ostacoli alla creazione di un vero mercato unico delle comunicazioni elettroniche. Il nuovo atto normativo, dovrebbe, ai sensi della consultazione, affrontare tali criticità attraverso un quadro giuridico più armonizzato, potenzialmente unificato in un unico strumento regolamentare che riassorba l'EECC, il regolamento BEREC, le norme sulla neutralità della rete e la politica europea sullo spettro radio[44].

È significativo osservare che la consultazione non menzioni il problema qui discusso della persistenza in vigore della direttiva *e-Privacy*. Tuttavia il tema della sua modifica, quando non direttamente della sua abrogazione, emerge come necessaria al fine di correggere l'attuale asimmetria regolamentare in molti dei contributi presentati dai soggetti che hanno partecipato alla consultazione[45].

---

[43] V. anche COMMISSIONE EUROPEA, *Libro bianco - Come affrontare adeguatamente le esigenze dell'Europa in termini di infrastruttura digitale?*, COM(2024) 81 final, Bruxelles, 21 febbraio 2024.

[44] L'iniziativa assume certamente una dimensione politico-strategica: la Commissione sembra infatti interpretare l'evoluzione delle reti digitali come un fattore essenziale per la competitività dell'Unione, la resilienza economica e la sicurezza, in linea con quanto emerso e sottolineato nei rapporti di Mario Draghi (*The Future of European Competitiveness - A Competitiveness Strategy for Europe*, presentato il 9 settembre 2024 ed Enrico Letta (*Much more than a Market - Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, presentato il 17-18 aprile 2024).

[45] V. in proposito i commenti inviati da Connect Europe, Telefónica S.A. (Spain), Liberty Global (Netherlands), Telenor Group (Norway), Telekom Austria AG - A1 Group (Austria) e Orange S.A. (France), nell'ambito della consultazione pubblica della Commissione europea sulla proposta di Digital Networks Act.

## 6. *Osservazioni conclusive*

Alla luce del quadro ricostruttivo svolto, la direttiva 2002/58/CE appare, sotto molti profili, ancorata a un contesto tecnologico e regolatorio ormai superato.

Ciò non toglie, tuttavia, che essa abbia svolto – e continui in parte a svolgere – una funzione importante nella protezione della riservatezza delle comunicazioni elettroniche. Da un lato, grazie all'elaborazione giurisprudenziale della Corte di giustizia, la direttiva *e-Privacy* è divenuta il perno di un sistema particolarmente avanzato di tutela della segretezza delle comunicazioni e dei c.d. metadati. Questo è avvenuto soprattutto grazie all'elaborazione di criteri molto rigorosi per le deroghe al regime di segretezza giustificate da esigenze di sicurezza nazionale o di contrasto ai reati. Dall'altro lato, la sua riforma del 2009 ha, come si è visto, anticipato istituti che sono poi confluiti nel GDPR: basti pensare all'obbligo di notifica delle violazioni di dati personali (*data breach*) agli utenti e alle autorità competenti, alla centralità della sicurezza delle reti e dei servizi come componente essenziale della tutela dei dati, nonché alla configurazione di un consenso informato, specifico e preventivo per l'uso dei terminali e delle tecnologie di tracciamento (la c.d. "cookie rule"), che costituirà il modello di riferimento per l'approccio successivo alla profilazione *online*.

La criticità più evidente riguarda il rapporto tra direttiva *e-Privacy* e GDPR.

Esso non può essere attualmente descritto in termini meramente lineari, come se la direttiva fosse una semplice *lex specialis* rispetto al regolamento qualificato come *lex generalis*. Le due fonti si collocano, piuttosto, in un rapporto che è in parte di specialità, in parte di integrazione e talvolta di sovrapposizione. Questo genera non poche incertezze nell'applicazione da parte degli operatori. Accanto alle aree in cui la direttiva specifica prevalendo sul quadro generale del GDPR – si pensi alle regole sui dati di traffico, sui dati di ubicazione o sull'accesso ai terminali – vi sono, infatti, ambiti in cui la disciplina settoriale integra il regolamento, estendendo la tutela anche alle persone giuridiche o a dati che, di per sé, non rientrerebbero nel perimetro del dato personale.

Al tempo stesso, la coesistenza di una fonte regolamentare direttamente applicabile e di discipline nazionali di recepimento della direttiva, crea una "specialità" che nella sostanza è tra norme di ordinamenti diversi. Il che sommato alla pluralità di autorità potenzialmente coinvolte nell'*enforcement*, contribuisce a disegnare un paesaggio frammentato, nel quale il confine tra prevalenza, integrazione e sovrapposizione non è sempre agevole da tracciare.

In questo quadro, uno dei nodi centrali è rappresentato dalla generalizzazione del consenso esplicito e preventivo quale presupposto di liceità dei trattamenti effettuati dai fornitori di reti e servizi di comunicazione elettronica. La direttiva e-*Privacy*, in linea con l'impostazione originaria della direttiva 95/46/CE, costruisce buona parte della tutela sull'idea di un consenso fortemente formalizzato, sia per l'utilizzo dei dati di traffico e di ubicazione, sia per l'accesso ai terminali. Tale scelta, se da un lato assicura un elevato grado di autodeterminazione informativa agli interessati – soprattutto rispetto alle forme di tracciamento e di marketing diretto più invasive – dall'altro si confronta con un modello, quello del GDPR, che ha riequilibrato il ruolo del consenso, affiancandogli in modo più netto ulteriori basi giuridiche del trattamento e invitando a un'applicazione meno "consenso-centrica" del sistema.

Ancora più marcata è la distanza rispetto agli atti del c.d. decennio digitale europeo, che pongono al centro la circolazione e la riutilizzabilità dei dati (personali e non personali) – pur entro cornici di garanzia – per finalità sia economiche sia sempre più apertamente funzionali alla garanzia dei diritti fondamentali[46].

Il risultato è una asimmetria regolamentare non irrilevante, soprattutto se la si osserva dal punto di vista concorrenziale: i fornitori tradizionali di servizi di comunicazione elettronica restano vincolati a un regime di consenso preventivo particolarmente stringente, mentre i molti fornitori di servizi digitali *over-the-top* operano sulla base di equilibri normativi in cui l'interesse legittimo e al-

[46] Sia consentito rinviare a M. Orofino, *The New Balance Between Data Circulation and Data Protection in the Digital Single Market*, in I. Anrò, F. Rossi Dal Pozzo (a cura di), *Il mercato unico digitale, tra antichi problemi e nuove sfide*, Fascicolo Speciale, 2025, Eurojus.

tre basi giuridiche (come ad esempio il contratto) trovano un terreno più ampio, con effetti potenzialmente distorsivi sul *level playing field*.

Il fallimento del progetto di regolamento e-*Privacy* ha lasciato questa situazione sostanzialmente immutata. Dopo anni di negoziati infruttuosi, la decisione della Commissione di ritirare la proposta appare, sotto certi aspetti, una presa d'atto di un mutato contesto: nel frattempo, il settore delle comunicazioni elettroniche ha perso parte della sua originaria specificità, inserendosi in un ecosistema digitale in cui reti, servizi di comunicazione, piattaforme e applicazioni convivono e competono nello stesso spazio di mercato, spesso offrendo funzionalità sostitutive.

Insistere su un regolamento settoriale concepito su una distinzione netta tra "operatori di comunicazione elettronica" e "altri fornitori di servizi digitali" rischiava probabilmente di cristallizzare una dicotomia che la realtà tecnologica e industriale aveva già superato. In questo senso, l'abbandono del progetto di riforma non è solo un indice di difficoltà politica, ma anche il sintomo di una tensione concettuale tra un approccio categoriale di matrice telco e una realtà in cui le comunicazioni elettroniche sono ormai una componente diffusa e trasversale del sistema digitale.

Resta allora la domanda, inevitabile, su quale debba essere il futuro della disciplina della riservatezza nelle comunicazioni elettroniche. Una possibile strada – sostenuta da numerosi attori del settore – è quella dell'abrogazione della direttiva e-*Privacy* e della sua piena integrazione in un quadro giuridico più armonizzato e orizzontale. Questa opzione appare a chi scrive percorribile ad un'unica condizione: che venga salvaguardato il principio fondamentale della segretezza delle comunicazioni, garantito dalle Costituzioni, dagli artt. 7 e 8 della Carta e dalla Corte di giustizia.

Questo principio, che costituisce il nucleo duro della direttiva e-*Privacy* fin dalla sua adozione ed è stato progressivamente rafforzato dalla giurisprudenza della Corte di giustizia, dovrebbe essere preservato e al tempo stesso integrato in un *framework* unitario che si applichi in modo eguale a tutti i fornitori di servizi di comunicazione, indipendentemente dalla qualifica formale e dalla tecnologia utilizzata.

Un tale intervento potrebbe avvenire, *de iure condenso*, sia con il *Digital Omnibus* (che in parte prevede l'abrogazione di singole norme della direttiva e-*Privacy*), sia con il *Digital Networks Act* ricomponendo le regole sulla riservatezza delle comunicazioni, sugli obblighi di sicurezza e sulle condizioni di accesso ai terminali, lungo l'intera filiera dei servizi di comunicazione digitale. Solo seguendo questa strada sarà possibile superare l'attuale frammentazione, garantire un equilibrio più coerente tra tutela dei diritti fondamentali e circolazione dei dati e, soprattutto, assicurare che il principio di segretezza delle comunicazioni continui a svolgere la sua funzione di presidio sostanziale della libertà individuale nell'ecosistema digitale contemporaneo.

FEDERICO GUSTAVO PIZZETTI

# DISPOSITIVI MEDICI, NEURODATI E DIRITTI FONDAMENTALI: VERSO UNA NUOVA REGOLAZIONE EUROPEA PER LE NEUROTECNOLOGIE?

SOMMARIO: 1. Le neurotecnologie e i neurodati alla frontiera dell'innovazione nella società digitale. – 2. Neurotecnologie, neurodati e diritti fondamentali. La "*Raccomandazione dell'Unesco sull'Etica della Neurotecnologia*". – 3. La conformità del vigente quadro europeo, applicabile (anche) alle neurotecnologie e ai neurodati, rispetto alla "*Raccomandazione dell'Unesco sull'Etica della Neurotecnologia*". – 4. Considerazioni conclusive.

## 1. *Le neurotecnologie e i neurodati alla frontiera dell'innovazione nella società digitale*

Tra le più significative frontiere dell'innovazione scientifica e tecnologica che caratterizzano l'epoca contemporanea e che sono capaci di dischiudere scenari di grande speranza ma altresì di determinare rischi di non trascurabile portata, si collocano – pare di potersi così affermare – gli avanzamenti conseguiti nel campo delle neuroscienze[1] e delle relative neurotecnologie[2].

[1] Fondamentali per l'inquadramento della disciplina risultano E.R. KANDEL, J.F. KOESTER, S.H. MACK, S.A. SIEGELBAUM, A.J. HUDSPETH, M. MATELLI, *Principi di neuroscienze*, V ed. it., Bologna, 2023; C. UMILTÀ, *Il cervello*, Bologna, 2007; C. UMILTÀ (a cura di), *Manuale di neuroscienze*, Bologna, 1999; R.F. THOMPSON, *Introduzione alle neuroscienze*, trad. it, Bologna, 1997; A. OLIVERIO, *Prima lezione di neuroscienze*, II ed., Bari-Roma, 2008; C. BERNASCONI, S. GARAGNA, G. MILANO, C.A. REDI, M. ZUCCOTTI (a cura di), *Neuroscienze. Itinerario fra tecnologia, etica e diritto*, Pavia, 2010; M. PICCOLINO (a cura di), *Neuroscienze controverse. Da Aristotele alla moderna scienza del linguaggio*, Torino, 2008; P. GRASSI, A. AGUTI (a cura di), *La natura dell'uomo. Neuroscienze e filosofia a confronto*, Milano, 2008; M.R. BENNETT, PM.S. HACKER, *Philosophical Foundations of Neuroscience*, Oxford, 2003.

[2] Cfr. G. SCOTT, *The neurotechnology revolution has arrived*, in *The Futurist*,

Secondo una definizione recentemente accolta in autorevole sede sovranazionale[3], con il termine "*neurotecnologie*" si intendono – in ampia accezione – tutti quei *dispositivi*, *sistemi* e *procedure idonei a interagire direttamente con il sistema nervoso umano* (centrale, periferico o enterico) *mediante lo scambio di segnali elettromagnetici* (quali le onde cerebrali) *o biochimici* (quali la componente ematico-dinamica delle aree cerebrali).

Volendo tracciare una carrellata senza pretesa alcuna di esaustività, si tratta di un ampio spettro di tecnologie che va da dispositivi che richiedono di essere direttamente *impiantati* nel tessuto cerebrale mediante l'effettuazione di operazioni di neurochirurgia (si pensi, a titolo esemplificativo, ai "*pacemaker* cerebrali") a macchinari in grado di svolgere le loro funzioni anche rimanendo all'*esterno* della scatola cranica (come la risonanza magnetica o la tomografia assiale computerizzata) sino a "*device*" che necessitano di essere *indossati* dall'utente e quindi di essere posti a contatto diretto col corpo ma in modo temporaneo e senza lo svolgimento di operazioni di innesto (tra i quali si annoverano i sempre più diffusi "caschetti" o "auricolari" ad onde cerebrali, dotati di tecnologie dedicate)[4].

Vi sono, inoltre, neuro-dispositivi costruiti e impiegati per "*captare*" i segnali provenienti dal sistema nervoso umano allo scopo di condurre analisi anatomofisiologiche (fra cui la risonanza magnetica funzionale, la tomografia a emissione di positroni o la spettroscopia funzionale nel vicino infrarosso); apparecchi in grado di "*manipolare*" in modo selettivo e mirato l'attività elettrochimica del cervello incrementandola[5] o inibendola (come accade con i neuro-stimolatori

---

2013, v. 47(5), p. 6; A. Roskies, *Neuroethics for the new millennium*, in *Neuron*, 2002, 35, pp. 21-23.

[3] Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), *Recommendation on Responsible innovation in neuroechnology*, OECD/LEGAL/0457, approvata l'11 dicembre 2019, in particolare §II, 6° alinea.

[4] Committee on Bioehtics (DH/BIO) del Consiglio d'Europa, *Common human rights challenges raised by different applications of neurotechnologies in the biomedical field*, rapporto sviluppato da M. Ienca, Strasbourg, 2021, pp. 11-22.

[5] Cfr. D.C. Turner, B.J. Sahakian, *Neuroethics of cognitive enhancement*, in *BioSocieties*, 2016, 1(1), pp. 113-123.

profondi, trans-cranici od opto-genetici)[6] e congegni che permettono di instaurare un vero e proprio *collegamento diretto*[7] *bidirezionale* tra il *cervello umano* e un *apparato digitale* esterno (quale un personal computer, uno *smartphone*, un *tablet* o un dispositivo di comunicazione, di locomozione o di volo: si tratta delle cosiddette interfacce cervello-computer)[8].

I neuro-dispositivi possono, poi, funzionare in modo "preimpostato" dal fabbricante o dall'utente (si tratta dei cosiddetti sistemi "*open-loop*") oppure mediante una costante "auto-modulazione" in tempo reale, effettuata dal macchinario sulla base del rilevamento, in continuo, degli stati psico-fisici dell'utilizzatore (sono i cosiddetti sistemi "*closed-loop*")[9].

---

[6] Cfr., per una disamina delle tecniche in questione, S. Sremic, A. Krsek, L. Baticic, *Deep Brain Stimulation: Psychological and Neuroethical Perspectives*, in *Neurol. Int.*, 2025, 17(10)(158), pp. 1-16; B. Dell'Osso (a cura di), *Brain stimulation in psichiatria. Tecniche ed impiego di TMS, tDCS, VNS e DBS*, Pisa, Pacini, 2022; E.S. Boyden, *Optogenetics and the future of neuroscience*, in *Nat. Neurosci.*, 2015, 18(9), pp. 1200-1201; Aa.Vv., *Moving magnetoencephalography towards real-world applications with a wearable system*, in *Nature*, 2018, v. 555(7698), pp. 657-661; S. Bode, A.H. He, C.S. Soon, R. Trampel, R. Turner, J.D. Haynes, *Tracking the unconscious generation of free decisions using uitra-high field Fmri*, in *Plos-one*, 2011, 6(6), n. e21612, pp. 1-13.

Per l'analisi dei profili etico-giuridici sollevati da questi apparecchi si segnalano: N.A. Vincent, *Neurolaw and Direct Brain Interventions*, in *Criminal Law and Philosophy*, 2014, v. 8, pp. 43-50; M. Sosa Navarro, S. Dura-Bernal, *Human Rights Systems of Protection from Neurotechnologies That Alter Brain Activity*, in *Drexel L. Rev.*, 2023, 15, pp. 893-942.

[7] Cfr. J.J. Vidal, *Toward direct brain-computer communication*, in *Annu. Rev. Biophys. Bioeng.*, 1973, 2, pp. 157-180.

[8] Cfr., per l'analisi tecnica, D. Braff, *New Wave: Wearable Neurotech Devices Are Becoming More Prevalent - Is the Law behind the Curve?*, in *Business of Law: Technology ABA Journal*, 2025, 111(2), pp. 9-11; S.K. Mudgal, S.K. Sharma, J. Chaturvedi, A. Sharma, *Brain Computer Interface Advancement in Neurosciences: Applications and Issues*, in *Interdiscip. Neurosurg.*, 2020, 20, n. 100694, pp. 1-8.

Si v. per i profili etico-giuridici relativi all'uso di tali macchinari: C. Conrad, C. A. Heggie, *Legal and Ethical Challenges Raised by Advances in Brain-Computer Interface Technology*, in *Can. J.L. & Tech.*, 2024, 21, pp. 201-215.

Per gli aspetti inerenti alla comunicazione con pazienti in stato di compromissione delle piene facoltà cognitive al fine di formulare diagnosi più accurate e di permettere loro una qualche manifestazione esteriore di volontà, si v. J.L. Haushalter, *Neuronal Testimonial: Brain-Computer Interfaces and the Law*, in *Vand. L. Rev.*, 2018, 71, pp. 1365-1400 (2018).

[9] Per la descrizione delle tecnologie in parola cfr. M. Carè, M. Chiappalone, V. Rosa Rota, *Personalized strategies of neurostimulation: from static to adaptive, open- to*

Molteplici sono gli usi e le finalità per i quali i diversi neuro-dispositivi qui accennati possono essere progettati, fabbricati e commercializzati. Nell'*ambito medico*, ad esempio, i neuro-dispositivi, sono utilizzati a fini di sperimentazione clinica, prevenzione, diagnosi, cura e riabilitazione di disturbi neurologici, oppure per la mitigazione o la compensazione di disabilità neuro-funzionali o neuro-sensoriali *non* altrimenti risolvibili.

Nel settore *non medico*, invece, i neuro-dispositivi in questione, per lo più di tipo indossabile[10], sono usati anche da soggetti *privi di menomazioni o patologie neurologiche* per un variegato insieme di attività fra le quali lo svolgimento di esperienze di gioco in scenari maggiormente immersivi; la navigazione in ambienti di realtà virtuale più sofisticati; l'auto-valutazione della stanchezza mentale o dei ritmi del sonno e della veglia; la gestione di dispositivi interattivi per la domotica; il controllo di *personal computer* o di *smartphone*; l'effettuazione di forme di comunicazione aumentata o di videoscrittura avanzata a impulsi neuronali[11]; il pilotaggio di apparecchi di ultima generazione per la mobilità; l'apprendimento intensivo mediante segnali cerebrali rilevati o indotti; la misurazione dei livelli di *stress* sul posto di lavoro (in particolare, nell'esecuzione di attività che richiedono carichi cognitivi notevoli o che implicano rischi elevati per la sicurezza); il miglioramento del benessere percepito o della concentrazione mentale; la rilevazione delle preferenze di consumo[12].

---

*closed-loop*, in *Front. Neurosci.*, 2024, 18, n. 1363128, pp. 1-14; L. Haag, G. Starke, M. Ploner, M. Ienca, *Ethical gaps in closed-loop neurotechnology: a scoping review*, in *NPJ Digit. Med.*, 2025, 8, n. 510, pp. 1-14.

[10] Con riferimento ad una promettente tecnologia di neuro-immagine che può essere utilizzata per l'analisi dei correlati neurali di stati mentali cfr. F.X. Shen, F. Lawrenz, S.M. Wolf, *Revolutionizing Neuroimaging Research with Highly Portable MRI: Confronting Ethical and Legal Challenges*, in *J.L. Med. & Ethics*, 2024, 52(764), pp. 764-768.

[11] Sia consentito il rinvio a F.G. Pizzetti, *Libertà di autodeterminazione e protezione del malato nel "Brain-Computer interfacing": un nuovo ruolo per l'amministratore di sostegno?*, in *Riv. crit. dir. priv.*, 2011, 1, pp. 31-59 e, più recentemente, a N. Liv, *Neurolaw: Brain-Computer Interfaces*, in *U. St. Thomas J.L. & Pub. Pol'y*, 2021, 15(1), pp. 328-355.

[12] Cfr. S. Salardi, *Neurotecnologie tra potere e libertà. Medicina, etica, discriminazione di genere*, Milano, 2024.

Tutti i *neuro-dispositivi*, inoltre, *indipendentemente* dalle *caratteristiche strutturali* (impiantabili, esterni o indossabili), dalle *funzionalità d'uso* (monitorare, modificare o interfacciare l'attività neurale) o dall'*ambito di impiego* (medico o *non* medico), si nutrono di peculiari tipi di *dati*, definiti, in sede sovranazionale[13], "*neurodati*" (o "*dati neuronali*" o "*dati personali cerebrali*")[14].

Si tratta, in specifico, di dati relativi alla *struttura anatomica* (si pensi ad una risonanza magnetica o ad una radiografia encefalica) oppure al *funzionamento* (si pensi ad un tracciato elettroencefalografico) *del sistema nervoso umano* (principalmente, del cervello), nonché di dati inerenti agli "*stati mentali*" *interni della persona*[15] (quali emozioni, cognizioni, volizioni, percezioni e ricordi[16]) ricavati dall'*attività neuro-biologica del cervello* secondo specifici rapporti di "correlazione"[17], scientificamente dimostrati, fra segnale cerebrale e stato psicologico (in altri termini, si inferisce, sulla base di determi-

---

[13] Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), *Recommendation on Responsible innovation in neuroechnology*, cit., in particolare § II, 5° alinea.

[14] Per una recente e interessante ricostruzione della disciplina giuridica applicabile ai neurodati riferita all'ordinamento europeo in comparazione col diritto cileno, si rinvia a M.I. Cornejo-Plaza, R. Cippitani, V. Pasquino, *La protezione giuridica dei "neurodati": i neurodiritti*, in *federalismi.it*, 2025, 2, pp. 165-185. Si v., inoltre, per una riflessione sulla protezione dei neurodati cerebrali che tiene in considerazione le più recenti innovazioni legislative introdotte nella *data protection law* americana, J.G. Browning, *Are Technology and the Law on the Same "Wavelength"?: Examining the New Frontier of Brainwaves and Data Privacy*, in *N.C.J.L. & Tech.* 2025, 26(345), pp. 345-390.

[15] Va, peraltro, avvertito che, oltre ai *neurodati*, vi sono anche dei *dati biometrici non neuronali*, dai quali, attraverso l'impiego di dispositivi e *software non* strettamente neuro-tecnologici, è possibile trarre *informazioni indirette* sull'attività mentale del soggetto. I riferimenti, a titolo esemplificativo, sono al tracciamento oculare, alla video-oculo-grafia, alla dinamica di digitazione, al riconoscimento vocale, all'analisi dell'andatura, alla conduttanza cutanea, alla variabilità della frequenza cardiaca, al monitoraggio dei movimenti durante il sonno, alla misurazione della pressione arteriosa, ai sistemi di mappatura delle emozioni facciali, all'indagine del micro-bioma.

[16] Illustrano gli avanzamenti sulla possibilità di ricavare contenuti mnestici dall'analisi dei dati neuronali E.R.D. Murphy, J. Rissman, *Evidence of Memory from Brain Data*, in *J.L. & Biosciences*, 2020, 1, pp. 1-58.

[17] Office for Democratic Institutions and Human Rights (ODIHR) dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), *Think Again: Freedom of Thought in the Age of Artificial Intelligence. Policy Brief*, Parigi., 2025, pp. 39-40.

nate caratteristiche morfologiche o di specifici *pattern* di attivazione cerebrale, rilevati dal neuro-dispositivo, il contenuto di pensiero che il soggetto potrebbe esperire in quel momento)[18].

## 2. *Neurotecnologie, neurodati e diritti fondamentali. La "Raccomandazione dell'Unesco sull'Etica della Neurotecnologia"*

Come ampiamente evidenziato in dottrina[19], il ricorso ai neuro-dispositivi, così come le operazioni di trattamento dei neurodati, proprio in quanto coinvolgono – lo si è visto[20] – il cervello e la

[18] Per gli aspetti tecnici si v. R.A. Poldrack, *Inferring mental states from neuroimaging data: from reverse inference to large-scale decoding*, in *Neuron*, 2011, 72(5), pp. 692-697; A. Omurtag, H. Aghajani, H.O. Keles, *Decoding human mental states by whole-head EEG+fNIRS during category fluency task performance*, in *J. Neural. Eng.*, 2017, 14(6), n. 066003, pp. 1-15.

Per l'analisi dei profili etici e giuridici nella prospettiva del riconoscimento di nuovi neuro-diritti, G. Belisario, *Neurodiritti: nuovi diritti o diritti già esistenti?*, in *federalismi.it*, 2024, pp. 69-87; M. Ienca, *Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti*, in *Not. Politeia*, 2019, 35, p. 53; C.M. Gillan, R.B. Rutledge, *Smartphones and the Neuroscience of Mental Health*, in *Annu. Rev. Neurosci.*, 2021, 8(44), pp. 129-151.

[19] Cfr., *ex multis*, A. D'Aloia, M.C. Errigo (a cura di), *Neuroscience and Law. Complicated Crossings and New Perspectives*, Cham, 2020; M. Ienca e R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, in *Life Sci., Soc. Policy*, 2017, 13(5), pp. 1-27; M. Ienca, *On neurorights*, in *Front. Hum. Neurosci.*, 2021, 15, n. 701258, pp. 1-11; G. D'Alessandro, F. Cirillo, *Neurodiritti: prospettive critiche e questioni dogmatiche*, in R. Torino, S. Zorzetto (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, pp. 93-132; S. Goering, E. Klein, L. Specker Sullivan *et al.*, *Recommendations for Responsible Development and Application of Neurotechnologies*. in *Neuroethics*, 2021, 14(3), pp. 365-386; N. Herts, *Neurorights - Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought*, in *Neuroethics*, 2023, 16(5), pp. 1-15; F. Cirillo, *Il fondamento costituzionale dei neurodiritto*, in *Rivista del Gruppo di Pisa*, 2021, f.s. 3, pp. 107-122; C. Stark, *Is a Global Governance Framework Necessary for Neurotechnology?*, in *Drexel L. Rev.*, 2023, 15(4), pp. 757-768; Aa.Vv., *Minding Rights: Mapping Ethical and Legal Foundations of "Neurorights"*, in *Camb. Q. Healthc. Ethics*, 2023, 32(4), pp. 461-481; J.C. Bublitz, *What an International Declaration on Neurotechnology and Human Rights Could Look Like: Ideas, Suggestions, Desiderata*, in *AJOB Neuroscience*, 2024, 15(2), pp. 96-112; E. Evgenyevna Gulyaeva, F. Farinella, *Human Neuro-Rights*, in *Quaestio Iuris* 2022, 15, pp. 278-299; F.G. Pizzetti, *Neurodiritto*, in A. Lavazza e V.A. Sironi (a cura di), *Neuroetica. Interpretare e orientare la rivoluzione delle neuroscienze*, Roma, 2022, pp. 105-117.

[20] V. *supra*, § 1.

mente umani, sono in grado di influire su tutta un'ampia gamma di *diritti individuali*.

Non è un caso, da questo punto di vista, che diversi siano stati i tentativi sinora intrapresi, tanto a livello internazionale[21], quanto nazionale[22], per tentare di definire un insieme di regole giuridiche specificamente dedicate alle neurotecnologie e ai neurodati, nonché

---

[21] Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), *Recommendation on Responsible innovation in neutoechnology*, OECD/LEGAL/0457, cit.; Human Rights Council delle Nazioni Unite (UN), *Res.* 51/3. *Neurotechnology and human rights*, approvata il 13 ottobre 2022, A/HRC/RES/51/2; Human Rights Council delle Nazioni Unite (UN), *Impact, opportunities and challenges of neurotechnology with regard to the promotion and protection of all human rights*, varato l'8 agosto 2024; Inter-American Juridical Committee dell'Organizzazione degli Stati Americani (OAS), *Inter-American Declaration of Principles regarding Neuroscience, Neurotechnologies and Human Rights*, approvata il 9 marzo 2025, CJI/RES 281; Consiglio europeo (UE), *León Declaration on European neurotechnology: a human focused and rights' oriented approach* proclamata durante una riunione informale a livello ministeriale il 24 ottobre 2023.

Si v., per un'analitica panoramica della disciplina internazionale relativa ai neurodiritti, M. Sosa Navarro, *The Role of Soft Law in the Regulation and Governance of Human Rights Challenges Posed by Neurotechnology*, Torino, 2025.

[22] In Francia, l'art. 16-14 del Codice civile stabilisce che le tecniche di neuro-immagine possono essere utilizzate, su di un individuo, solo per scopi di ricerca medica o scientifica, oppure in ambito forense (escluse, in quest'ultimo caso, le neuro-immagini funzionali), previo consenso esplicito e revocabile del soggetto, prestato a fronte di adeguata informazione ricevuta. Il legislatore francese ha, quindi, dettato disposizioni che riguardano non solo, e non tanto, i neurodati, quanto anche, e piuttosto, l'applicazione delle neurotecnologie in ambito *extra-sanitario* fissando un divieto di utilizzo delle neuro-immagini (ad esempio, la risonanza magnetica e la risonanza magnetica funzionale, la tomografia assiale computerizzata, ma *non* l'elettro-encefalografia, che restituisce solo un tracciato grafico e *non* una "immagine") ritenendo queste ultime maggiormente a rischio di indurre nei terzi atteggiamenti sviati o erronei in danno dei soggetti ai quali le immagini stesse si riferiscono in virtù del grado di risoluzione "topografica" che le stesse immagini raggiungono circa la struttura e l'attività cerebrale, oltreché per il potenziale "evocativo" e "suggestivo" che le immagini vantano rispetto a più "crudi" e "freddi" dati alfanumerici.

In Spagna, sia pure soltanto a livello di disciplina di *soft-law* destinata alle amministrazioni dello Stato, la nuova Carta dei diritti digitali, all'art. XXVI, comma 1, prevede il riconoscimento del diritto dell'individuo alla sua identità personale e alla sua autonomia decisionale rispetto alle neurotecnologie, e ribadisce il diritto dello stesso soggetto alla protezione dei dati tratti dal funzionamento del suo sistema nervoso. Lo Stato iberico ha, quindi, inteso accomunare, nella medesima "linea guida" offerta all'Amministrazione pubblica, entrambi i profili che la regolazione delle neurotecnologie pone sotto il proprio cono di attenzione: quello dei neurodati, da una parte,

per provare ad individuare e tutelare nuovi "*neurodiritti*"[23] della persona umana direttamente legati alle tecnologie e ai dati in questione.

---

rispetto alla garanzia di un elevato livello di protezione, e quello dei neurodiritti, dall'altra parte, soprattutto in relazione all'uso delle neurotecnologie alteranti l'identità e l'autonomia individuali. Il medesimo articolo XXVI della Carta spagnola, al successivo comma 2, fa riferimento alla legge dello Stato (ovviamente, a titolo non vincolante, essendo la Carta in questione priva di valore costituzionale) quale fonte appositamente adatta a regolare, nel rispetto dei princìpi di dignità della persona e di non discriminazione in conformità ai trattati e alle convenzioni internazionali, i casi e le condizioni di utilizzo delle neurotecnologie per il potenziamento umano.

In America Latina, il novellato art. 19, sez. I, della Costituzione cilena prevede la protezione, da parte dello Stato, sia dell'attività cerebrale dell'individuo, sia delle informazioni che da essa se ne possono trarre ponendo tale tutela nell'ambito del diritto, di rango costituzionale, alla libertà psico-fisica e rimettendo alla legge l'individuazione delle condizioni, dei requisiti e dei limiti d'uso delle neurotecnologie.

Negli Stati Uniti, l'art. 1798.140 del Codice civile della California e l'art. 6-1-1303 del Testo Unico delle leggi del Colorado riconoscono la natura di "dati sensibili" ai "dati neuronali" – questi ultimi intesi quali informazioni generate dalla rilevazione dell'attività del sistema nervoso centrale di un individuo – al fine di assoggettare i dati in questione alla più severa tutela prevista per le informazioni "sensibili", ivi compresa l'applicazione delle regole, dal contenuto più rigoroso, stabilite per il consenso al trattamento e per la raccolta e conservazione di tali dati "sensibili" anche dal punto di vista della predisposizione di adeguate misure di sicurezza. Emerge, dunque, nella prospettiva statunitense, l'attenzione rivolta, nei due stati federali, alla protezione rafforzata del "neuro-dato" personale piuttosto che alle modalità di fabbricazione, commercializzazione e impiego delle neurotecnologie in relazione ad altri diritti fondamentali. Giova, peraltro, osservare che, a livello *federale*, non esiste una disciplina appositamente rivolta alla regolazione delle neurotecnologie: il trattamento dei neurodati resta, dunque, sottoposto all'applicazione della HIPAA *Rule*, mentre per quanto riguarda i dispositivi in grado di interagire con il cervello nel *campo medico*, si applica la comune FDA *Regulation*.

In Italia, al momento, il legislatore ha adottato – come noto – un'apposita disciplina nazionale relativa all'*intelligenza artificiale* [nel quadro della normativa europea di cui al regolamento (UE) n. 2024/1689], costituita dalla legge 23 settembre 2025, n. 132 ma non ha inteso pervenire ad una normativa "di settore" anche per le neurotecnologie. Ne consegue che le previsioni della legge n. 132 del 2025 troveranno applicazione anche ai dispositivi neuro-tecnologici unicamente nella misura in cui questi ultimi, oltre ad essere impiegabili nei settori disciplinati dalla legge in parola, contengano anche un sistema di intelligenza artificiale. Per contro, norme dettate anche alle neurotecnologie, e non solo all'intelligenza artificiale, sono contenute in due progetti di legge di identico tenore, n. C. 2121 (Ascani *et al.*) e n. S. 1245 (Basso *et al.*), tuttora in corso d'esame in Commissione.

[23] Cfr., in particolare, le ampie e preziose riflessioni di G. De Minico, *Nuova tecnica per nuove diseguaglianze. Case law: Disciplina Telecomunicazioni, Digital Services Act e Neurodiritti*, in *federalismi.it*, 2024, n. 6, pp. 6-10.

Particolare rilevanza assume, in questa prospettiva, la recentissima "*Raccomandazione sull'Etica della Neurotecnologia*" (di seguito, semplicemente "*Raccomandazione*")[24], approvata dall'Unesco l'11 novembre 2025 nel corso della XLIII riunione della Conferenza generale dell'Organizzazione internazionale[25] tenutasi a Samarcanda[26].

La *Raccomandazione*, infatti, costituisce il più aggiornato e ampio catalogo di regole giuridiche ed etiche[27] formulato a livello globale[28] per indirizzare gli Stati nella regolazione dello sviluppo delle neurotecnologie e nel trattamento dei neurodati in modo pienamente rispettoso della *dignità* e dei *diritti fondamentali*[29] dell'*essere umano*.

---

[24] Organizzazione delle Nazioni Unite per l'educazione, la Scienza e la Cultura (UNESCO), *Draft Recommendation on the Ethics of neurotechnology*, n. SHS/IGM-NEURO/2025/MAY/3, pp. 1-26 (or. inglese e francese), formulata il 12-16 maggio 2025 a Parigi dal gruppo intergovernativo di esperti di II livello dell'Unesco, successivamente inviata dal Direttore generale agli Stati membri mediante lettera circolare n. CL/4513 l'11 luglio 2025 e infine presentata, il 24 luglio 2025, alla Conferenza Generale con il n. 43 C-30, pp. 1-27 (or. inglese) sulla base del mandato attribuito allo stesso Direttore generale, con atto n. 42C/Resolution 29, dalla Conferenza tenutasi a Parigi dal 7 al 22 novembre 2023.

[25] Sia permesso riferirsi a F.G. Pizzetti, *In quest of constitutional principles of neurolaw*, in *Med. Secoli*, 2011, 23(3), pp. 963-990 e più recentemente, rispetto al ruolo che l'Unesco poteva svolgere nella "codificazione" dei neurodiritti e da prima ancora che l'Organizzazione avviasse ufficialmente il procedimento che ha portato al varo della disciplina etico-giuridica sulle neurotecnologie, a F.G. Pizzetti, *A proposal for a "Universal Declaration on Neuroscience and Human Rights"*, in *Bioethical Voices (Newsletter of the UNESCO Chair of Bioethics*), 2017, 6(10), pp. 3-6.

[26] La *Risoluzione*, che sarà pubblicata entro il 12 gennaio 2026, dovrà essere siglata dal Direttore generale dell'UNESCO entro sei mesi e sarà tramessa alle Autorità competenti di tutti gli Stati membri dell'Organizzazione internazionale.

[27] Cfr. V.A. Sironi, M. Di Francesco (a cura di), *Neuroetica. La nuova sfida delle neuroscienze*, Roma-Bari, 2011; G. Corbellini, E. Sirgiovanni, *Tutta colpa del cervello. Un'introduzione alla neuroetica*, Milano, 2013; N. Levy, *Neuroetica. Le basi neurologiche del senso morale*, Milano, 2009; L. Boella, *Neuroetica. La morale prima della morale*, Milano, 2007; M.J. Farah, *Neuroetica. Le implicazioni morali, legali e sociali delle neuroscienze*, Milano, 2010.

[28] Per un'attenta riflessione sull'opportunità di prevedere un sistema di regole internazionali sulle neurotecnologie, cfr. C. Stark, *Is A Global Governance Framework Necessary for Neurotechnology?*, in *Drexel L. Rev.* 2025, 15, pp. 757-767.

[29] Cfr. A. Facchi, S. Falcetta, N. Riva, *An Introduction to Fundamental Rights in Europe*, Cheltenam, Elgar, 2022.

Più in specifico, la *Raccomandazione* – che combina[30] il "*rights-based approach*"[31], il "*context-based approach*"[32] e il "*science-based approach*"[33] – si articola in sei parti: la prima, dedicata all'introduzione delle definizioni di sistema nervoso, neuro-tecnologia e neuro-dati e all'individuazione dell'ambito di applicazione della Raccomandazione (che comprende le neuro-tecnologie per uso medicale e non medicale e ogni attività che riguardi misurazione, registrazione, la modificazione e la modulazione dell'attività del sistema nervoso umano, nonché i relativi trattamenti dati) (§§ 1-19); la seconda, rivolta alla fissazione degli scopi e degli obiettivi della Raccomandazione fra i quali spiccano la protezione delle libertà e dei diritti fondamentali, la promozione dell'uguaglianza, dell'inclusione e della non discriminazione, l'incentivo allo sviluppo sostenibile e scientificamente fondato e altresì all'uso responsabile delle neuro-tecnologie (§§ 20-21); la terza, comprendente l'enucleazione di valori e princìpi fondamentali in relazione alla ricerca, sviluppo e uso delle neuro-tecnologie fra cui la dignità umana, l'inclusione, la salute psico-fisica, l'autonomia individuale e la libertà cognitiva, la protezione dei neurodati, l'affidabilità e la trasparenza, l'*accountability*, la salvaguardia dei diritti dei soggetti vulnerabili e l'adozione di modelli di valutazione dell'impatto delle neuro-tecnologie centrati sull'essere umano (§§ 24-69); la quarta, contenente la previsione di

[30] Di interesse nell'analisi sistematica dei modelli regolatori è M.R. O'Shaughnessy, W.G. Johnson, L. Nalbach Tournas. C.J. Rozell, K.S. Rommelfanger, *Neuroethics guidance documents: principles, analysis, and implementation strategies*, in *J. Law Biosci.*, 2023, 10(2), n. lsad025, pp. 1-19.

[31] Cfr. Consiglio europeo (UE), *León Declaration on European neurotechnology: a human focused and rights' oriented approach*, cit., ispirata all'approccio basato sui diritti fondamentali nella regolazione delle nuove tecnologie del cervello.

[32] Cfr. Steering Committee for Human Rights in the fields of Biomedicine and Health Bioehtics (CDBIO) del Consiglio d'Europa, *Neurotechnologies and Human Rights. Do We Need New Rights?*, Council of Europe pub., 2022, spec. p. 18, in cui si sottolinea l'opportunità di adottare discipline "flessibili" che si adattino alla peculiarità dei diversi contesti d'impiego delle neuro-tecnologie e dei relativi soggetti che se ne servono.

[33] Organizzazione per la Cooperazione e lo Sviluppo Economico (OECD), *Neurotechnology Toolkit. To support policymakers in implementing the OECD Recommendation on Responsible Innovation in Neurotechnology*, Parigi, 2025, che raccomanda lo sviluppo della collaborazione scientifica nel campo delle neuro-tecnologie.

apposite regole giuridiche (e linee di *policy*) in materia di investimenti, uso e regolazione pubblica delle neuro-tecnologie, *governance* dei neurodati, *cyber*-sicurezza, ricerca scientifica e applicazioni mediche, alfabetizzazione digitale, eguaglianza di genere, istruzione, lavoro e usi commerciali dei neuro-dispositivi nonché in relazione all'uso delle neuro-tecnologie per finalità di neuro-potenziamento (§§ 70-156); la quinta, costituita dai meccanismi di implementazione, a livello nazionale, delle previsioni internazionali (ivi compreso il ruolo di supporto dell'Unesco mediante l'adozione di standard metodologici per la valutazione etica d'impatto delle neuro-tecnologie) (§§ 157-164); la sesta, che raccoglie le disposizioni finali (§§ 165-166).

Fermando, in questa sede, l'attenzione su alcuni solamente degli aspetti ritenuti di particolare interesse della *Raccomandazione*, giova, sin da subito, evidenziare la peculiare centralità che viene, da quest'ultima, attribuita al fondamentale valore della *dignità umana*[34] intesa quale *intrinseco e pari valore di ogni essere umano* al cui sviluppo le *neurotecnologie devono tendere* sulla base di un *approccio "antropocentrico"* (§ 24), attento anche al benessere delle *future generazioni* (in quanto ritenute sviluppo dell'umanità stessa) (§ 65 e § 69).

Diffusamente si sofferma, poi, la Raccomandazione sui princìpi di *eguaglianza e non discriminazione* auspicando che l'accesso ai benefici derivanti dall'avanzamento delle neurotecnologie avvenga mediante un sistema di regole e di incentivi introdotto dagli Stati in modo da *ridurre* le diseguaglianze nei livelli di salute oggi esistenti con particolare (ma non esclusivo) riferimento ai Paesi ancora in via di sviluppo (§§ 28-29 e §§ 66-68).

La *Raccomandazione* richiede, in proposito, agli Stati, di adoperarsi affinché le neurotecnologie *non* cristallizzino, né amplifichino forme già esistenti di discriminazione fondate su caratteristiche neurologiche o mentali ma al contrario rafforzino l'identità e la varietà

[34] Cfr. E. García-López, J.M. Muñoz, R. Andorno, *Editorial. Neurorights and Mental Freedom: Emerging Challenges to Debates on Human Dignity and Neurotechnologies*, in *Front. Hum. Neurosci.*, 2021, n. 823570; Cfr. E. Moreu Carbonell, *The Regulation of Neuro-Rights*, in *Eur. Rev. Digit. Adm. Law*, 2021, pp. 149-162.

culturale, nonché la neuro-diversità individuale[35] e la parità di genere (§ 30, §§ 51-52 e §§ 101-103).

Agli Stati è altresì richiesto di sostenere la ricerca aperta e condivisa in campo neuro-scientifico, anche nella prospettiva di ridurre così l'ammontare dei costi dei neuro-dispositivi posti a carico dei cittadini (§§ 81-82 e § 112).

Per quanto concerne – poi – il *diritto alla salute e all'integrità psico-fisica*[36] – di indubbio rilievo, dato che i neuro-dispositivi agiscono, in molti modi diversi, sul cervello e il sistema nervoso dell'individuo – la *Raccomandazione* afferma che la ricerca, lo sviluppo e l'applicazione delle neurotecnologie debbono avere, quale loro principale obiettivo, il *non* arrecare *danni evitabili* all'essere umano secondo la regola generale del "*do not harm*" (§ 40).

Gli Stati sono, di conseguenza, tenuti a varare discipline che incentivino la diffusione di neurotecnologie sicure e basate su prove scientifiche rigorose dando priorità agli scopi preventivi, diagnostici, terapeutici, riabilitativi e assistenziali idonei ad apportare benefici al più alto numero possibile di persone (§§ 25-26, §§ 39-42, §§ 71-72 e §§ 104-105).

Gli stessi Stati sono, inoltre, tenuti a istituire (o, se necessario, a rafforzare) meccanismi di controllo aventi l'obiettivo di valutare l'impatto sulla salute psico-fisica, nonché sulla socializzazione, derivante dall'uso, in particolare a lungo termine, di apparecchi neurotecnologici (§ 29, § 106 e § 107).

Per quanto riguarda, poi, più in particolare, i profili di tutela e di promozione dell'integrità psicofisica legati all'uso dei neuro-dispositivi *medici* la *Raccomandazione* invita gli Stati ad adottare regole che incentivino la progettazione e la fabbricazione di neuro-apparecchi per uso medicale che siano il più possibile affidabili, si-

---

[35] Cfr. A. Lollini, *Brain Equality: Legal Implications of Neurodiversity in a Comparative Perspective*, in *N.Y.U. J. Int'l L. & Pol.*, 2018, 51, pp. 69-133.

[36] Cfr. C. Bublitz, *Neurotechnologies and Human Rights: Restating and Reaffirming the Multi-Layered Protection of the Person*, in *Int'l J. Hum. Rts.*, 2024, 28(5), pp. 782-807; S. Barbareschi, *Rivoluzione digitale e diritti dei disabili: la tecnologia come fattore inclusivo e la tutela dell'habeas mentem*, in *Rivista del Gruppo di Pisa*, 2021, pp. 299-311; S. Fuselli, *Neurotecnologie e tutela dell'integrità psichica. Profili costituzionali e sovranazionali*, in *J. Ethics Leg. Technol.*, 2020, 2(1), pp. 1-28.

curi e durevoli; richiedano una manutenzione minima; abbiano un'obsolescenza tecnologica contenuta; assicurino un'assistenza continua nel tempo anche nel caso in cui i produttori non siano più in grado di prestarla (§§ 107-108).

La *Raccomandazione*, inoltre, sollecita gli Stati a implementare (o a irrobustire, laddove esistenti) sistemi di monitoraggio interoperabili dei neuro-dispositivi medicali in modo da tenere debita traccia degli effetti collaterali negativi da essi cagionati, anche mediante la raccolta di informazioni provenienti dal personale medico e dai pazienti (§ 109).

Per quel che concerne, invece, i neuro-dispositivi *non* medicali, la commercializzazione dovrebbe avvenire, stando alla *Raccomandazione*, in forza di regole nazionali che contemplino appositi obblighi per il produttore di proteggere gli utenti da diversi tipi di rischi per la salute, compresi quelli di natura psicologica; di fornire un'informazione chiara, comprensibile e basata su prove scientifiche solide circa i rischi (e i benefici) per la salute connessi all'impiego degli apparecchi in vendita escludendo affermazioni fuorvianti o suggestive; di effettuare rigorose prove di sicurezza, tossicità ed efficacia con un'adeguata supervisione medica qualora il prodotto, pur non destinato all'uso sanitario, dichiari comunque di trattare, prevenire o diagnosticare malattie oppure condizioni di carattere medicale (§ 133).

Per quel che attiene – poi – al *diritto all'autodeterminazione individuale e alla libertà "di" pensiero*[37] – invero cruciale quando,

[37] Quando si accede ai meccanismi interni del cervello, come le neuroscienze mirano a rendere possibile, non è, infatti, soltanto la libertà "di *manifestazione*" del pensiero che va salvaguardata ma altresì, e prima ancora, la stessa *libera* "*formazione*" *del pensiero* da parte dell'individuo. Cfr., nell'ampia bibliografia sul tema, J.M. Muñoz, J.A. Marinaro, *"You Shall Have the Thought": Habeas Cogitationem as a New Legal Remedy to Enforce Freedom of Thinking and Neurorights*, in *Neuroethics*, 2024, 17(1), pp. 1-22; S. Lighart, *Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity*, in *ECHR Law Rev.*, 2024, 5(2), pp. 199-229; P. Sommaggio, M. Mazzocca, A. Gerola, F. Ferro, *Cognitive liberty. A first step towards a human neuro-rights declaration*, in *BioLaw J./Riv. bio-dir.*, 2017, 3, pp. 27-45; W. Sententia, *Neuroethical considerations: cognitive liberty and converging technologies for improving human cognition*, in *Ann. N.Y. Acad. Sci.*, 2004, 1013(1), pp. 221-228; J.C. Bublitz, R. Merkel, *Crimes against minds: On mental manipulations, harms and a human right to mental self-deter-*

come nella specie, la tecnologia intrude nell'intimo foro del cervello e degli stati mentali individuali[38] – la *Raccomandazione* impone agli Stati di proteggere l'integrità mentale del soggetto da qualsiasi interferenza considerata indesiderata e dannosa (§§ 43-44), nonché di assicurare, con apposita disciplina, che le persone siano messe in grado di assumere decisioni libere, informate e volontarie sull'eventuale ricorso alle neurotecnologie di qualsiasi tipo esse siano (§ 45).

Cardine è, in punto, la regola del "*consenso informato*" da prestarsi, in base alle discipline nazionali, sempre (e solo) in via *preventiva* da parte dell'interessato, secondo il modello dell'"*opt-in*", dopo aver ricevuto elementi informativi completi e comprensibili, nonché "tarati" in relazione all'età, alle condizioni mentali e al livello di istruzione (§ 46).

In tale ottica, gli Stati, oltre ad introdurre obblighi informativi specifici in sede di acquisizione del consenso all'uso della singola neurotecnologia, dovrebbero promuovere forme di alfabetizzazione generale sulle neurotecnologie nel loro complesso anche mediante strumenti di diffusione, quali siti Internet dedicati oppure eventi aperti alla cittadinanza con il coinvolgimento di esperti (§ 97, § 99).

Nei casi in cui ci si trovi di fronte a persone incapaci, gli Stati debbono prevedere, in base alla *Raccomandazione*, che il consenso informato sia prestato dal *rappresentante legale* dell'infermo o del minore rispettando, quanto più possibile, i desideri manifestati dalla persona non capace, in relazione all'età o all'attitudine al discernimento (§ 46).

Il consenso informato deve, comunque, prevedere, secondo le regole nazionali, anche lo speculare *diritto di rifiutare* o *revocare*, in qualsiasi momento, l'impiego del neuro-dispositivo (§ 46).

A maggior protezione dell'autonomia cognitiva e volitiva dell'individuo rispetto a perniciose forme di condizionamento perpe-

---

*mination*, in *Criminal Law and Philosophy*, 2017, 8(1), pp. 51-77; A. Pirozzoli, *La libertà di coscienza e le neuroscienze cognitive*, in *Consulta on-line*, 2020, pp. 1-7; A. Lavazza, *Manipolare la memoria. Scienza ed etica della rimozione dei ricordi*, Milano, 2013; T. Istace, *Neurorights: The Debate about New Legal Safeguards to Protect the Mind*, in *Issues Law Med.*, 2022, 37(95), pp. 95-109; S. Ligthart, *The Right to Mental Integrity in the Age of Neurotechnology: Constructing Scope and Permissible Limitations*, in *J.L. & Biosciences*, 2025, 12(1), n. lsaf010, pp. 1-23.

[38] V. *supra*, § 1.

trate mediante captazione o alterazione di segnali cerebrali, la *Raccomandazione* richiede agli Stati di prevedere che le neurotecnologie *non* siano mai utilizzate, né da parte di enti pubblici, né da parte di soggetti privati, allo scopo di esercitare un'*influenza indebita* o una *manipolazione insidiosa* in danno dell'individuo (§ 47). Del tutto escluso, da parte delle legislazioni nazionali, deve anche essere il ricorso ai neuro-dispositivi al fine di esercitare *forme coercitive di adeguamento dei comportamenti individuali*, soprattutto sul piano politico, sociale, religioso oppure per instaurare forme di *controllo sociale* o ancora per espletare attività di *sorveglianza arbitraria o illegittima degli stati mentali individuali* (§ 75).

Per quanto attiene – poi – al *diritto alla protezione dei dati neuronali*[39] – di palmare importanza in relazione alla già menzionata natura dei dati in questione di essere ricavati dal cervello (e dal sistema nervoso) dell'individuo[40] – la *Raccomandazione* afferma che i neurodati debbano considerarsi *non* soltanto appartenenti alla categoria dei dati "personali" ma altresì sempre riconducibili alla tipologia dei dati cosiddetti "*sensibili*": destinati, in quanto tali, a ricevere, da parte degli ordinamenti nazionali, una tutela specifica e rafforzata (§ 48 e § 85).

In base alle normative che Stati dovranno appositamente adottare, quindi, qualsiasi trattamento di dati neuronali va sottoposto alla regola del *consenso informato*, *anticipato* e *libero* dell'interessato, fatta eccezione per le situazioni di emergenza medica, in cui il soggetto si trovi in pericolo di vita (§ 49).

Gli Stati devono, altresì, vietare le pratiche che subordino l'accesso a beni o servizi al conferimento di dati neurali (in quanto si

---

[39] Cfr. P. Kellmeyer, *Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices*, in *Neuroethics*, 2021, 14, pp. 83-98; F. X. Shen, *Neuroscience, Mental Privacy, and the Law*, in *Harv. J.L. & Pub. Pol'y*, 2017, 36, pp. 653-713; J.G. Browning, *Are Technology and the Law on the Same "Wavelength"?: Examining the New Frontier of Brainwaves and Data Privacy*, in *N.C. J.L. & Tech.*, 2025, 26(3), pp. 345-390; P.R. Wolpe, *Neuroprivacy and Cognitive Liberty*, in Aa.Vv., *The Routledge Handbook of Neuroethics*, Routledge, 2017, pp. 214-224; J. Ryberg, *Neuroscience, Mind Reading and Mental Privacy*, in *Res Publica*, 2017, 23, pp. 197-211; W. Unger, *Stay Out of My Head: Neurodata, Privacy, and the First Amendment*, in *Wash. & Lee L. Rev.*, 2023, 80, pp. 1439-1521.

[40] V. *supra* § 1.

tratterebbe di consenso fortemente condizionato e quindi non più pienamente libero), o che usino gli stessi dati, persino in *assenza di valido consenso*, per forme di pubblicità mirata (§ 86).

Gli stessi Stati sono, altresì, tenuti a prevedere misure rigorose di salvaguardia dei dati neurali, nonché di contrasto al trattamento improprio o *non* autorizzato dei dati medesimi (§ 50), anche prevedendo modelli specifici di "*governance dei neurodati*" così da assicurare il pieno ed effettivo rispetto dei principi di liceità, minimizzazione, anonimizzazione, pseudonimizzazione e proporzionalità (§§ 85-86).

Agli Stati è, inoltre, richiesto, sempre dalla *Raccomandazione*, di incentivare, mediante apposite regole (e politiche pubbliche), lo sviluppo e l'attuazione di innovazioni tecnologiche e di standard di progettazione che migliorino la protezione dei dati neurali, fra i quali la crittografia d'avanguardia, le banche dati con autenticazione a più fattori, le tecniche di anonimizzazione di ultima generazione e le pratiche di elaborazione e archiviazione dei dati in prossimità del luogo in cui i dati stessi sono generati (§§ 88-89 e §§ 93-95).

La tutela accordata dalla *Raccomandazione* ai dati personali cerebrali *non* esclude, peraltro, che gli stessi Stati siano anche chiamati a *promuovere* la *circolazione* transfrontaliera dei neurodati, con particolare riguardo al *settore della ricerca scientifica*, mediante la condivisione di archivi e il ricorso a strumenti sicuri da attacchi informatici e rispettosi dei principi di minimizzazione dei dati e di riuso per finalità eticamente lecite (§§ 90-91).

Riconoscendo, in particolare, l'importanza che la circolazione dei neurodati può avere nello specifico *campo dell'addestramento dell'intelligenza artificiale* (soprattutto se di tipo generativo), la *Raccomandazione* invita, altresì, gli Stati ad adottare apposite regole giuridiche (e linee guida etiche) per assicurare che il riuso dei dati neurali nelle attività di ricerca e sviluppo dei sistemi di IA escluda la ricorrenza di "*bias*"; comprenda la supervisione umana; implichi l'esecuzione di test rigorosi così da assicurare qualità e integrità dei dati impiegati per il "*deep-learning*" e il "*machine-learning*" (§ 92 e § 114).

Non basta. La *Raccomandazione* si sofferma – infatti – anche su alcuni *ambiti particolari* di *impiego delle neurotecnologie* e di *trattamento dei neurodati*, rispetto ai quali l'Unesco ha ritenuto oppor-

tuna, a fini di piena tutela dei diritti e della dignità delle persone coinvolte, l'enunciazione di regole e misure peculiari.

Nel *contesto educativo*[41], infatti, la *Raccomandazione*, pur considerando che il ricorso alle neurotecnologie può assicurare un miglior godimento dei diritti all'istruzione e alla formazione, richiede nondimeno agli Stati di vigilare con attenzione sui pericoli che l'applicazione indiscriminata di neuro-dispositivi può comportare, specialmente in relazione allo sviluppo psicologico e cognitivo dei discenti, e soprattutto quando si tratta di persone *non* affette da disabilità o disturbi neurologici (§§ 118).

Va in ogni caso garantito, in forza di apposite norme adottate dagli Stati, che l'utilizzo di neuro-dispositivi nelle aule scolastiche avvenga solo sulla base di dati scientifici, nonché in linea con gli obiettivi educativi e in via *complementare* (e *non* alternativa) ai metodi tradizionali di apprendimento (§ 119).

Agli Stati è, poi, richiesto di prevedere regole che assicurino che qualsiasi implementazione di neurotecnologie nei confronti degli alunni sia subordinata al *previo consenso informato* dei genitori (o tutori) prestato dopo un adeguato periodo di riflessione e con *divieto* di applicare incentivi o penalità in relazione al rilascio, o al mancato rilascio, del consenso stesso (§ 121).

Gli Stati devono vietare qualsiasi ricorso alla neurotecnologia per la *valutazione* delle *prestazioni* degli studenti o degli insegnanti (§§ 121).

È infine, caldeggiata, dalla *Raccomandazione*, la creazione, a livello nazionale, di organismi amministrativi indipendenti aventi il compito di verificare periodicamente, insieme agli esponenti delle categorie interessate, i profili di sicurezza e di rischio legati all'impiego di neuro-dispositivi sugli alunni (§§ 122).

In *ambito forense*[42], poi, se l'eventuale ricorso a mezzi di prova di tipo neuro-tecnologico consente al prevenuto di poter esercitare

---

[41] Di particolare interesse, anche per l'analisi dei più recenti sviluppi, risulta il contributo di J. Sanabria, Z.M. Cebral-Loureda, J.M. Antelis, S. Lee, *Advances in complex thinking and neurotechnologies in education: a bibliometric analysis of research trends*, in *Cong. Process.*, 2025, pp. 611-624.

[42] Sul quale sia permesso rinviare a F.G. Pizzetti, *Neuroscienze forensi e diritti fondamentali: spunti costituzionali*, Torino, 2012. Più recentemente, cfr. C. Grandi,

in modo ancor più effettivo il *diritto alla difesa ed alla prova* di cui gode (ad esempio, mediante il ricorso a sofisticate perizie sulla capacità di intendere e di volere o di ricordare correttamente e completamente i fatti), tanto il *principio del giusto processo*, da una parte, quanto il *diritto fondamentale a non autoincriminarsi*, dall'altra, *non* consentono agli Stati – lo sottolinea bene la *Raccomandazione* – di prevedere l'impiego di neuro-dispositivi o il trattamento di neurodati allo scopo di estrarre (laddove possibile), dalla mente dell'imputato stesso (al di sotto della sua soglia di coscienza e volontà), elementi che possano contribuire ad affermarne la colpevolezza (§ 74). Ogni uso di neuro-tecnologie nell'ambito dei procedimenti giudiziari deve basarsi su solide evidenze scientifiche e prevedere, per legge, l'adozione di istituti e meccanismi di controllo rigorosi che includano anche la protezione dei dati e la tutela della libertà morale dei soggetti coinvolti (§ 74).

Per quel che attiene – poi – al *settore del lavoro*[43], la *Raccomandazione* sollecita gli Stati a introdurre regole specifiche affinché l'impiego di neuro-dispositivi e il trattamento dei neurodati da parte dei datori di lavoro avvengano non soltanto a fronte di evidenze scientifiche consolidate, ma altresì su *base esclusivamente volontaria* tenendo in debito conto la condizione di subordinazione del prestatore d'opera che potrebbe minare la genuinità del consenso. È comunque richiesta la previa somministrazione da parte del datore di lavoro di un'informazione trasparente e accurata sulla tipologia e sugli effetti del dispositivo impiegato, nonché sulla qualità, modalità e durata della raccolta dei neurodati (§ 124).

Resta, peraltro, fermo che gli Stati devono garantire che ogni attività di trattamento dei neurodati dei lavoratori avvenga solo per una finalità legittima attinente alla sicurezza o alla salute dei lavoratori medesimi o dei terzi con i quali essi vengono in contatto (§ 124).

---

*Neuroscienze e responsabilità penale. Nuove soluzioni per problemi antichi?*, Torino, 2016; F. Stocchi, *Neuroscienze e applicazioni in ambito forense: profili filosofici ed etico-giuridici*, Torino, 2025; E. Sirgiovanni, G. Corbellini, C. Caporale, *A recap on Italian neurolaw: epistemological and ethical issues*, in *Mind & Society*, 2017, 16, pp. 17-35.

[43] Cfr. E. Muhl, R. Andorno, *Neurosurveillance in the workplace: do employers have the right to monitor employees' minds?*, in *Front. Hum. Dyn.*, 2023, pp. 1-11, nonché, con attente osservazioni, F. Di Tano, *Neurodiritti e dati neurali verso una tutela giuridica*, in *Labour Law Issues*, 2025, 1, pp. 1-20.

I lavoratori devono, inoltre, essere sottoposti a un'adeguata formazione concernente l'uso delle neurotecnologie e le misure erette a protezione dei dati neuronali nel contesto in cui prestano l'attività lavorativa (§ 126).

Gli Stati *non* devono in nessun caso permettere, secondo quanto la *Raccomandazione* stabilisce, che le neurotecnologie possano essere implementate in azienda (e i relativi neurodati trattati) al fine di *valutare* la *performance* del lavoratore o di irrogare *sanzioni disciplinari*, oppure con modalità che compromettano la salute del lavoratore o ne consentano la profilazione individuale, oppure ancora in tutti i casi in cui i rischi d'uso del neuro-dispositivo superano i benefici attesi (§ 124).

Si specifica, inoltre, che le legislazioni nazionali devono assicurare che sia fatto divieto, ai datori di lavoro, di trattare dati neuronali dei dipendenti al di fuori dell'orario o del luogo di lavoro (ad esempio, disattivando automaticamente la raccolta dati). Parimenti deve essere inibito, agli stessi datori di lavoro, di avere accesso a dati neuronali dei lavoratori che, diversi da quelli inerenti la prestazione lavorativa dedotta, siano stati raccolti incidentalmente dal neuro-dispositivo indossato durante lo svolgimento della mansione. Né dovrebbe essere ritenuta lecita – salvo l'espresso consenso del lavoratore – la trasmissione dei neurodati a soggetti terzi non dipendenti del datore di lavoro o non legati all'esecuzione della prestazione lavorativa oggetto del contratto di assunzione (§ 125 e § 128).

Secondo quanto la Raccomandazione stabilisce, inoltre, gli Stati devono prevedere, con apposite norme, che i neurodati raccolti durante l'attività lavorativa, unitamente alle analisi su di essi effettuate dal datore di lavoro, vengano messi a disposizione del lavoratore qualora questi ne faccia richiesta. In ogni caso di cessazione del rapporto di lavoro, il datore di lavoro deve, comunque, provvedere alla restituzione di tutti dati in questione al lavoratore, oppure alla loro integrale, e automatica, cancellazione (§ 127 e § 129).

La *Raccomandazione* richiede, poi, agli Stati di adottare regole puntuali che tutelino le persone in cerca di lavoro dallo sfruttamento e dalla discriminazione limitando, in specifico, le ipotesi di ricorso all'uso delle neurotecnologie per l'assunzione e altresì adeguando le normative esistenti (o sviluppandone di nuove) in mate-

ria di utilizzo dei dati neuronali per la profilazione del posto di lavoro (§ 131).

Nei settori del *commercio* e del *consumo*[44] – poi – la *Raccomandazione* richiama i legislatori nazionali all'adozione di discipline in grado di individuare un corretto punto di equilibrio fra lo sviluppo e la commercializzazione di dispositivi neuro-tecnologici per uso *ludico-ricreativo* o per lo svolgimento di altre *attività quotidiane della persona*, da una parte, e il rispetto dei *diritti fondamentali dell'individuo*, dall'altra, con particolare attenzione alla *salute fisica e mentale*, all'*autodeterminazione consapevole* e alla *protezione dei neurodati* (§ 132).

Peculiare attenzione è dedicata, in specie, al *divieto* di ricorrere alle pratiche di "*tying*" consistenti nella richiesta, rivolta all'utente dall'impresa, di consentire al trattamento dei dati neuronali quale indispensabile requisito per poter accedere a specifici beni in commercio o a determinati servizi offerti, anche su siti Internet (§ 133).

A fronte dei rischi che l'uso improprio (o illecito) dei neuro-dispositivi può determinare su taluni consumatori, in modo particolare rispetto all'eccitazione di circuiti cerebrali coinvolti nell'insorgere di forme di dipendenza (il richiamo e, segnatamente, ai sistemi dopaminergici), la *Raccomandazione* impegna gli Stati ad adottare regole che impediscano la commercializzazione di neuro-dispositivi in grado di sfruttare artatamente le condizioni di vulnerabilità di speciali categorie di persone (quali gli individui affetti da ludopatia) (§ 138).

Anche attraverso appropriate informazioni al pubblico, gli Stati devono, inoltre, promuovere un uso consapevole, da parte dei cittadini, dei neuro-dispositivi con particolare riguardo per quegli apparecchi in grado di effettuare la *stimolazione cerebrale* per *scopi non medicali* (dati gli effetti che tali apparecchi potrebbero determinare sul cervello e il sistema nervoso di soggetti sani) (§ 138).

La *Raccomandazione* invita, inoltre, gli Stati ad adottare regole per proteggere l'autonomia e la riservatezza dei consumatori da pratiche suggestive o manipolatorie che si servano di neurotecnolo-

[44] Cfr. S. Rainey, J.C. Bublitz, H. Maslen, H. Thornton, *Data as a cross-cutting dimension of ethical importance in direct-to-consumer neurotechnologies*, in *AJOB Neuroscience*, 2019, 10(4), pp. 180-182.

gie (e di neurodati) per il funzionamento dei "*sistemi di raccomandazione*" o per lo svolgimento di attività di "*priming*" e di "*nudging*" anche in Rete (con esclusione degli scopi, comunque *non* manipolatori, di incentivazione di comportamenti virtuosi in ambito medico, e sempre subordinatamente al consenso espresso da parte del soggetto) [§ 140, lett. *a*) e *b*)].

Va, in ogni caso, vietata – a livello di legislazione nazionale – l'attività di *marketing*[45], ivi compresa quella di natura politico-elettorale, che utilizzi neuro-dispositivi e raccolga neurodati *durante la fase del sonno* del soggetto[46] [§ 136, lett. *c*)].

La *Raccomandazione* contempla, infine, alcune misure "tarate" su taluni "gruppi di soggetti" considerati *fragili*[47].

Con riguardo alle persone *minorenni*, la *Raccomandazione* invita gli Stati ad adottare discipline specifiche per *prevenire* l'uso di tecniche di *neuro-marketing*[48] su bambini o adolescenti (§ 145).

Rispetto alle *persone anziane*[49], la *Raccomandazione* chiede agli Stati di valorizzare le iniziative, scientificamente fondate, che ab-

---

[45] Un'analisi approfondita dei profili rilevanti dell'uso delle neurotecnologie a fini di *marketing* con riferimento anche alla disciplina applicabile nell'Unione europea è stata compiuta da I. Geraci, *Il neuromarketing nel quadro giuridico europeo: riflessioni sulle opportunità e sui rischi per i soggetti vulnerabili*, in *Persona e Mercato*, 2024, n. 2, pp. 1169-1188. Di interesse è anche L. Sposini, *Impact of New Technologies on Economic Behavior and Consumer Freedom of Choice: From Neuromarketing to Neuro-Rights*, in *J. Digit. Technol. Law*, 2024, 1, pp. 85-87. Fondamentale, in tema, rimane lo studio di L. Tafaro, *Neuromarketing e tutela del consenso*, Napoli, 2018. Si v. anche, sul piano della potenzialità tecniche degli strumenti di captazione delle onde cerebrali per rilevare preferenze di consumo, A. Bazzani, S. Ravaioli, U. Faraguna, G. Turchetti, *Is EEG Suitable for Marketing Research? A Systematic Review*, in *Front. Neurosci.*, 2020, 14, p. 2. Più in generale, cfr. N. Bault, E. Rusconi, *The Art of Influencing Consumer Choices: A Reflection on Recent Advances in Decision Neuroscience*, in *Front. Psychol.*, 2020, 10, n. 3009, pp. 1-7.

[46] Cfr. T. Horikawa, M. Tamaki, Y. Miyawaki, Y. Kamitani, *Neural Decoding of Visual Imagery During Sleep*, in *Science*, 2010, 340(6132), p. 639.

[47] Cfr. A.A. Mollo, *La vulnerabilità tecnologica. Neurorights ed esigenze di tutela: profili etici e giuridici*, in *Eur. J. Priv. Law Tech.*, 2021, pp. 199-210.

[48] Cfr. S. Guida, *Affrontare il potere della neurotecnologia: Il neuromarketing tra azzardo morale, impatti sulla personalità dell'utente e tutela dei neurodiritti*, in *Eur. J. Priv. Law Tech.*, 2023, pp. 1-37.

[49] Per la ricostruzione delle potenziali strumentazioni tecniche e l'analisi dei profili etico-giuridici in relazione all'impiego di forme di potenziamento neuronale rispetto ai soggetti nella terza età, cfr. M. Ienca, D.M. Shaw, B. Elger, *Cognitive enhan-*

biano per obiettivo l'integrazione delle neurotecnologie negli ambienti di cura (§§ 146-148).

Con riferimento ai *soggetti portatori di disabilità*, la *Raccomandazione* esorta gli Stati ad adottare politiche che valorizzino il potenziale delle neurotecnologie nella rimozione degli ostacoli che le persone diversamente abili incontrano durante la loro vita professionale o negli spazi ricreativi (§ 149 e § 150).

Nei confronti dei soggetti con diagnosi di *disturbo mentale*, la *Raccomandazione* invita gli Stati a promuovere la ricerca scientifica e a sostenere iniziative rivolte ad affrontare le esigenze speciali che tali individui manifestano soprattutto attraverso la realizzazione, la diffusione e la sorveglianza post-commercializzazione di neurotecnologie dedicate al miglioramento delle funzioni psichiche compromesse (§§ 152-154).

Da ultimo, merita segnalare che la *Raccomandazione* suggerisce agli Stati di introdurre sia lo strumento della "*valutazione di impatto sui diritti umani*" al fine di identificare, prevenire e mitigare i possibili effetti negativi delle neurotecnologie sui diritti fondamentali della persona, sia l'istituto della "*valutazione di impatto sulla privacy*" in modo tale da rilevare e ridurre i pericoli, per la lesione della riservatezza dell'individuo, derivanti dai trattamenti dei suoi neuro-dati [§ 80, lett. *a*) e *d*)].

## 3. *La conformità del vigente quadro europeo, applicabile (anche) alle neurotecnologie e ai neurodati, rispetto alla "Raccomandazione dell'Unesco sull'Etica della Neurotecnologia"*

La *Raccomandazione* qui tratteggiata[50] ha efficacia – in termini di *soft-law* – verso tutti gli Stati parte dell'Unesco che saranno, di conseguenza, tenuti a metterla in pratica non solo adottando misure legislative e varando politiche pubbliche in base alle rispettive di-

---

*cement for the ageing world: opportunities and challenges*, in *Ageing and Society*, 2019, 39(10), pp. 2308-2321.

[50] V. *supra*, § 2.

[51] Cfr. F. Pizzetti, S. Calzolaio, A, Iannuzzi, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Torino, 2024.

sposizioni costituzionali, ma altresì istituendo o designando appositi organismi nazionali (§ 159 e § 160).

Come avvenuto in altri settori di "punta" della disciplina della società digitale[51], fra i quali i servizi digitali o l'intelligenza artificiale, l'Unione europea potrebbe, quindi, esser chiamata, a breve, a valutare l'eventualità di un proprio intervento normativo al fine di precludere ai singoli Stati Membri l'adozione di discipline interne, sporadiche e parziali, di recepimento dei princìpi e delle regole fissate dall'Organizzazione internazionale.

Tali iniziative messe in cantiere da parte degli Stati membri, potrebbero, infatti, compromettere, proprio per via della loro eterogeneità nazionale, il corretto e armonico funzionamento del mercato unico delle neuro-tecnologie a livello europeo.

D'altro canto, l'Unione europea ha sempre più spesso inteso porsi anche quale "faro" per illuminare la strada di un governo globale della società digitale in chiave antropocentrica e attenta ai diritti fondamentali della persona.

In tale prospettiva, la stessa Unione europea potrebbe, dunque, voler fungere da "apripista" anche rispetto alla disciplina, "di frontiera", delle emergenti tecnologie del cervello procedendo, prima di altri grandi attori geo-politici (americani o asiatici), al recepimento, su scala continentale, della *Raccomandazione* dell'Unesco.

Ove volesse procedere lungo tale direttrice, va rilevato che l'Unione europea sembra vantare un ampio ventaglio di regole di *diritto primario*[52] che, pur *mai* facendo esplicita menzione dell'innovazione neuro-tecnologica, appaiono assai "in asse" rispetto ai princìpi enucleati nella *Raccomandazione*[53].

È ben noto, infatti, quanto la *dignità umana*, cardine dell'impianto valoriale della *Raccomandazione*[54], costituisca anche "pietra angolare" dell'intero edificio giuridico-assiologico dell'Unione ai

[52] Si rinvia, per un'attenta analisi del quadro giuridico vigente di protezione dei diritti fondamentali a livello europeo applicabile agli sviluppi neuro-scientifici, a F. Cirillo, *Neurodiritti: ambiguità della "libertà cognitiva" e prospettive di tutela*, in *Consulta-online*, 2023, pp. 32-40.

[53] V. *supra*, § 2.

[54] V. *supra*, § 2.

sensi dell'art. 2 del Trattato sull'Unione europea e dell'art. 1 della Carta dei diritti fondamentali dell'Unione europea.

Il *diritto all'autodeterminazione e all'integrità mentale* poi – assunto come centrale nella *Raccomandazione*[55] – è esplicitamente riconosciuto e garantito, con particolare (ma non esclusivo) riguardo (proprio) ai settori della biologia e della medicina (in cui le neurotecnologie ricadono), dall'art. 3 della Carta dei diritti fondamentali dell'Unione europea.

Il *diritto alla protezione dei dati personali* – ampiamente affermato e salvaguardato dalla *Raccomandazione* dell'Unesco[56] – è sancito dall'art. 7 della Carta dei diritti fondamentali dell'Unione europea.

Il *diritto alla libertà "di" pensiero* – intesa quale facoltà di formare autonomamente i propri stati mentali senza manipolazioni arbitrarie altrui, su cui la *Raccomandazione* diffusamente si sofferma[57] – può ricondursi alla "*libertà di pensiero e di espressione*" scolpita dall'art. 10 della Carta dei diritti fondamentali dell'Unione europea.

Il *diritto alla salute* – che la *Raccomandazione* considera con peculiare attenzione[58] – è proclamato dall'art. 35 della Carta dei diritti fondamentali dell'Unione europea e ulteriormente rafforzato, quanto a divieto di discriminazione nell'equo accesso ai servizi, dall'art. 21 della Carta[59].

Va, invece, sottolineato che sussistono elementi di potenziale disallineamento fra le norme europee di *diritto derivato* applicabili *anche* alle neuro-tecnologie e ai neuro-dati, pur non essendo state concepite per tale disciplina, e le regole invocate dalla *Raccomandazione* per il governo delle neuro-tecnologie[60]. In particolare, vengono in rilievo, per le ragioni che si esporranno, i regolamenti europei in materia di protezione dati personali, dispositivi medici e intelligenza artificiale.

---

[55] V. *supra*, § 2.

[56] V. *supra*, § 2.

[57] V. *supra*, § 2.

[58] V. *supra*, § 2.

[59] Panel for the Future of Science and Technology del Parlamento europeo, *The protection of mental privacy in the area of neuroscience. Societal, legal and ethical challenges*, Bruxelles-Strasbourg, 2024, n. 757.807, pp. 44-45.

[60] V. *supra*, § 2.

In materia di protezione dati personali, è, invero, ben noto che il regolamento (UE) n. 2016/679 (GDRP)[61] trova applicazione, ai sensi dell'art. 2, par. 1, rispetto a ogni «trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi» (salvo talune eccezioni, enumerate ai paragrafi 2 e 3).

A norma del successivo art. 4, par. 1, num. 1), GDPR, è considerato "dato personale" «qualsiasi informazione riguardante una persona fisica identificata o identificabile» ritenendosi «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»[62].

Ora, considerati, per così dire, nel loro stato "grezzo" – vale a dire, di meri impulsi elettrochimici generati dal sistema nervoso

---

[61] Per una minima bibliografia, si v. V. Ricciuto (a cura di), *Il Regolamento europeo sulla protezione dei dati personali. Commentario al Reg. (UE) 2016/679*, Torino, 2019; A. Mantelero, *La protezione dei dati personali nell'era digitale. Regole, diritti e garanzie*, Torino, 2020; C. Kuner, *The General Data Protection Regulation: A Commentary*, 2nd ed., Oxford, 2020; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, v. I e v. II, Torino, 2016; G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017; R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021.

[62] Merita segnalare che la Commissione europea ha depositato, il 19 novembre 2025, una articolata *proposta di modifica* di diversi atti regolamentari incidenti sui trattamenti dati nel campo del digitale [COM(2025) 837, "*Digital Omnibus*"] nell'ambito della quale si interverrebbe anche sull'art. 4, num. 1, GDPR puntualizzando che *non* basta la "*mera identificabilità*" del soggetto, al quale il dato si riferisce, per rendere il dato in parola "personale" ai fini dell'applicazione della normativa regolamentare di protezione dati se un'altra persona fisica o giuridica *non* è in grado di identificare la persona fisica tenendo conto dei mezzi di cui potrebbe *ragionevolmente disporre* o del fatto che un potenziale *destinatario successivo* dispone di tali mezzi. Ove tale *proposta* venisse un domani approvata dal legislatore europeo, ne andrebbe, quindi, valutata la portata rispetto alla *Raccomandazione* dell'Unesco la quale prevede che i "neuro-dati" siano sempre considerati come personali, indipendentemente dalla realistica possibilità che essi costituiscano vettore di identificazione del soggetto dal cui cervello (e sistema nervoso) sono stati estratti e a prescindere dal fatto che l'identificazione costituisca lo scopo perseguito dal titolare del trattamento (v. *supra*, § 2).

umano e captati dai neuro-dispositivi – i neurodati *non* sembrerebbero, di per sé, *direttamente identificativi* di una persona fisica (salvo, ovviamente, che l'utente abbia dovuto registrarsi o accreditarsi per poter utilizzare l'apparecchio, oppure nel caso in cui il dato cerebrale sia stato "etichettato", sin dal momento iniziale in cui è stato raccolto, con i riferimenti anagrafici dell'interessato). I trattamenti dati neuronali risulterebbero, quindi, di primo acchito, *esclusi* dall'abito di applicazione del regolamento (UE) n. 2016/679 con tutto quel che ne consegue in punto di affievolita tutela dei diritti della persona.

Tuttavia, gli stessi dati neuronali, una volta che vengono elaborati, costituiscono le tessere di un mosaico unico, e preciso, dell'identità, neuro-fisiologica o neuro-psichica, del soggetto a cui essi pertengono (oltreché del suo profilo genetico).

Da questo punto di vista, perciò, se si pone mente alla giurisprudenza della Corte di giustizia dell'Unione europea[63], la quale ha esteso, in via interpretativa, la nozione di soggetto "identificabile" comprendendovi anche la *mera possibilità*, e non solo la *realistica plausibilità*, di identificazione, si può giungere a sostenere che i neurodati, in quanto collegabili a un individuo di cui riflettono informazioni fisiche, fisiologiche o psichiche, costituiscono – ancorché *non* espressamente menzionati nel GDPR – "dati personali" ai sensi e per gli effetti dell'art. 4 del regolamento (UE) n. 2016/679[64].

Si pone, di conseguenza, l'interrogativo se i neurodati, una volta considerati come "dati personali", possano esser fatti rientrare nella categoria dei dati "speciali" (c.d. "*dati sensibili*"), dotati di protezione rafforzata ai sensi dell'art. 9, GDPR, oppure se a essi si debba applicare la disciplina "generale" di cui all'art. 6, GDPR.

---

[63] Corte di giustizia dell'Unione europea, *Nowak v. Data Protection Commissioner*, C-434/16, CGUE [2017] e *Patrick Breyer v. Bundesrepublik Deutschland*, C-582/14, CGUE [2016].

[64] Per un'ampia analisi in punto applicabilità ai neurodati del regolamento (UE) n. 2016/679, cfr. S. Frischenbruder Sulzbach, *Protection of Neurodata in the European Union: Impacts of Emerging (Neuro) Technologies on the (Neuro)Privacy of the Data Subject*, in *Latin American Journal of European Studies*, 2023, 3(2), pp. 180-212, nonché M. Ienca, G. Malgieri, *Mental Data Protection and the GDPR*, in *J.L. & Biosciences*, 2022, 9(1), pp. 1-19.

In effetti, i neurodati potrebbero essere fatti rientrare nell'ambito di applicazione dell'art. 9, GDPR[65] quali «dati relativi alla salute»[66].

[65] Cfr. R. TREZZA, *La tutela della persona umana nell'era dell'intelligenza artificiale: rilievi critici*, in *federalismi.it*, 2022, p. 300 secondo la quale i neurodati sono sicuramente parte della categoria dei dati c.d. "sensibili".

[66] Merita, inoltre, considerare che, in materia di trattamento dei dati sulla salute, l'Unione europea si è, da ultimo, dotata di un sofisticato quadro di disciplina costituito dal regolamento (UE) n. 2025/327 sullo spazio europeo dei dati sanitari (EHDSR).

Ai limitati fini della presente riflessione, vale la pena osservare che il regolamento in questione ha lo scopo di «migliorare l'accesso delle persone fisiche ai loro dati sanitari elettronici personali e il loro controllo su tali dati nel contesto dell'assistenza sanitaria, nonché per conseguire più efficacemente altre finalità che comportano l'uso dei dati sanitari elettronici nei settori sanitario e assistenziale di cui beneficerebbe la società» fra le quali rientrano la ricerca, l'innovazione, la risposta a minacce sanitarie (pandemie comprese), la sicurezza dei pazienti e la medicina personalizzata [considerando n. 1)].

In particolare, il regolamento (UE) n. 2025/327, nel rispetto e in conformità ai valori dell'Unione, trova applicazione, specificando e integrando i diritti di cui al regolamento (UE) n. 2016/679, ai dati relativi alla salute, fisica o mentale e ai dati genetici trattati in formato elettronico, sia personali che non personali, compresi quelli che sono stati anonimizzati in modo tale da *non* riferirsi più a una persona fisica identificata o identificabile, che siano stati raccolti da *dispositivi medici* (o nello svolgimento di attività di ricerca clinica ed assistenza medica), oppure da *applicazioni per il benessere*, autonomamente utilizzate dagli individui [considerando n. 7) e articoli 1 e 2].

Per quanto *non contenga alcuna misura specificamente "ritagliata" sui dati sanitari di tipo "neuronale"* pare, però, ragionevole ritenere che i neurodati, se acquisiti per finalità di salute e se trattati in formato elettronico all'interno di un sistema di cartelle cliniche elettroniche interoperabili, ricadano nel campo di applicazione del regolamento (UE) n. 2025/237 quali "dati sanitari" rilevati da dispositivi medici o da applicazioni per il benessere.

Giova, in proposito, osservare che il regolamento (UE) n. 2025/327 *esclude* la necessità di ottenere il *consenso dell'interessato al trattamento dei dati sanitari per finalità di ricerca scientifica* avendo previsto (unicamente) il diritto all'"*opt-out*".

Si tratta di un elemento, questo, che, se applicato i neurodati, quali dati sanitari, mal si concilia con la "*Raccomandazione sull'Etica della Neurotecnologia*" dell'Unesco in base alla quale, invece, la circolazione transfrontaliera dei neurodati deve essere sempre subordinata all'*esplicito consenso* dell'interessato, reso sulla base di un'informazione somministrata in modo trasparente, completo e comprensibile (v. *supra*, § 2).

Rispetto ad altri aspetti legati alla condivisione e all'interoperabilità dei neurodati (assumendo questi ultimi all'interno nella categoria di "dati sanitari" a cui il regolamento si applica), lo stesso regolamento (UE) n. 2025/327 delinea, invece, una disciplina che appare assai coerente con la *Raccomandazione* dell'Unesco (v. *supra*, § 2).

Si stabilisce, infatti, che l'accesso ai dati sanitari personali per finalità di ricerca debba essere subordinato ad un'apposita autorizzazione, da rilasciarsi ad opera degli HDAB, e si indicano, altresì, le finalità rispetto alle quali è comunque fatto *divieto* di

I neurodati, infatti, se usati in ambito medico, sono in grado di rivelare *elementi pertinenti allo stato di salute della persona* con riferimento non solo alle patologie (o ai *deficit*) del cervello, ma altresì al funzionamento e alla morfologia "in salute" del sistema nervoso.

Tuttavia, come s'è in precedenza osservato[67], i dati neuronali possono essere raccolti e trattati, dai neuro-dispositivi, anche *al di fuori dell'ambito della ricerca scientifica o della pratica clinica* e per finalità che poco, o nulla, hanno a che vedere con la *salute dell'individuo*.

Si potrebbe, allora, sostenere – e non a torto – che *non* tutti i neurodati elaborati dai neuro-dispositivi ma *solo* quelli che vengono *trattati da neuro-dispositivi medici* per finalità di ricerca scientifica-medica o di trattamento sanitario ricadono nell'ambito speciale d'applicazione tracciato dall'art. 9, GDPR con conseguente riconduzione di tutti gli *altri* tipi di neurodati al quadro generale previsto dall'art. 6 GDPR.

Ebbene, al fine di estendere le più robuste misure di protezione contemplate dall'art. 9, GDPR *anche* ai neurodati *non* raccolti e trattati nel campo della *salute umana*, sulla scorta di quanto la *Raccomandazione* dell'Unesco auspica, si potrebbe far leva sull'essere i neurodati in questione dei «dati biometrici», *ex* art. 9, GDPR, in quanto oggetto di trattamenti tecnici specifici (quelli, cioè, posti in essere dai neuro-dispositivi) relativi a «caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica» *ex* art. 4, par. 1, num. 14), GDPR[68].

---

riuso dei dati sanitari personali, fra le quali rientrano l'adozione di eventuali decisioni pregiudizievoli per la persona fisica interessata; l'incremento dei premi assicurativi; la pubblicizzazione di prodotti o terapie; lo sviluppo di prodotti ritenuti dannosi per gli individui e per la società. Tutti scopi, questi, che risultano oggetto di limitazione o divieto anche nella Raccomandazione dell'Unesco rispetto ai trattamenti di neurodati (v. *supra*, § 2).

L'accesso ai dati dovrà, inoltre, avvenire, sempre secondo il regolamento (UE) n. 2025/327, in forma anonimizzata o pseudononimizzata e in un ambiente digitalmente sicuro, soggetto a misure tecniche e organizzative dettagliate e supervisionate. Misure, queste, che, di primo acchito, appaiono conformi ai parametri di cyber-sicurezza previsti, in specifico per i dati neuronali, dalla *Raccomandazione* dell'Unesco (v. *supra*, § 2).

[67] V. *supra*, § 1.

[68] Cfr. M. Ienca, G. Malgieri, *Mental data protection and the GDPR*, in *J.L. & Biosciences*, 2022, 9(1), pp. 3-4.

Non si può, tuttavia, non considerare, da questo punto di vista, che la categoria dei "dati biometrici", di cui all'art. 9, GDPR, se letta in combinato disposto con l'art. 4, par. 1, num. 14), GDPR, fa espresso riferimento al profilo, che tali dati biometrici devono necessariamente presentare, di essere *finalizzati* a permettere o confermare «l'identificazione univoca» del soggetto (come accade, ben è noto, coi rilievi dattiloscopici o con l'immagine facciale[69]).

Non tutti i dati neuronali sono, però, trattati allo scopo *specifico* di riconoscere o verificare l'identità di un soggetto, né tutti i neuro-dispositivi sono *tecnicamente progettati* per tale finalità (si pensi, ad esempio, ai neuro-dispositivi usati nella pratica clinica, oppure a quelli adoperati per il monitoraggio di funzioni cognitive, livelli di stress, stati mentali, o ancora a quelli di cui ci si serve per comandare *smartphone* o "*device*" computerizzati).

Non solo. La circostanza che i dati biometrici, per esser considerati tali, ai sensi degli artt. 4 e 9 del regolamento (UE) n. 2016/679, debbono potersi riferire a una "*caratteristica*" fisica, fisiologica o comportamentale *presumibilmente stabile* del soggetto (come è un'impronta digitale), potrebbe risultar d'ostacolo a ritenere che siano dati biometrici, e quindi "sensibili", tutti quei neurodati catturati da neurotecnologie che registrano solo *fluttuazioni dinamiche* dell'attività cerebrale *momento per momento* (come gli stati di sonno e di veglia, i livelli di attenzione, concentrazione o carico cognitivo, e così via).

Al fine di assicurare ai trattamenti dei neurodati quella tutela rafforzata dei diritti della persona che la Raccomandazione impone[70], si potrebbe, invero, tentare di ricondurre i neurodati in questione fra i dati "sensibili" di cui all'art. 9, GDPR sostenendo che tali tipi di dati, sia pure solo all'esito di complesse ed elaborate

---

[69] Significativo è, in tal senso, il considerando n. 51), GDPR, il quale, in relazione alla necessità di un nesso "stretto" fra la natura biometrica del dato e la finalità di permettere l'identificazione del soggetto al quale il dato si riferisce, ha sottolineato, ricorrendo all'esempio delle immagini fotografiche, che il «trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica».

[70] V. *supra*, § 2.

procedure di analisi e inferenza, potrebbero condurre a ricavare «opinioni politiche», «convinzioni religiose o filosofiche» o anche l'«orientamento sessuale» del soggetto, deducendoli, in qualche modo, dalla "mente".

Vale, però, la pena osservare che almeno allo stato attuale di sviluppo delle neuroscienze e delle neurotecnologie, pare piuttosto difficile che si riesca ad ottenere, dalla "lavorazione" di neurodati "grezzi", costrutti tanto articolati e complessi quali quelli che riguardano un'opinione politica, una convinzione filosofica o religiosa, oppure un'appartenenza ad un certo orientamento sessuale.

D'altra parte, se *non* appare così lontano il giorno in cui *anche* tali elementi potranno essere agevolmente "estrapolati" dal cervello, analizzandone gli impulsi mediante neuro-macchine, va comunque ricordato che la "*privacy mentale*" che la *Raccomandazione* dell'Unesco sollecita gli Stati a proteggere[71] *non* si limita alle *sole* opinioni politiche, convinzioni filosofiche, credo religioso, od orientamento sessuale[72].

Dal punto di vista della protezione assicurata ai dati neuronali, l'ordinamento vigente dell'Unione europea si presta, dunque, a una lettura "in chiaro-scuro" se posto a confronto con la disciplina etico-giuridica sulle neuro-tecnologie approvata dall'Unesco[73].

Da una parte, infatti, il regolamento (UE) n. 2016/679 sembra essere applicabile anche ai neurodati quali dati ritenuti personali[74] pur non senza incertezze nalla misura in cui manca, nella normativa europea, un preciso ancoraggio letterale che includa anche i neurodati nella categoria dei dati personali di cui all'art. 4, GDPR.

Dall'altra parte, è solo con non poche "torsioni" che la disciplina di cui al regolamento (UE) n. 2016/679 ritenuta applicabile può essere pienamente adattata al principio, a chiare lettere affermato dalla *Raccomandazione* dell'Unesco, in forza del quale i neuro-

---

[71] V. *supra*, § 2.

[72] Cfr. A. Safron, V. Klimaj, S. Sylva, A. Rosenthal, M. Li, M. Walter, J.M. Bailey, *Neural correlates of sexual orientation in heterosexual, bisexual, and homosexual women*, in *Sci. Rep.*, 2018, 8(1), pp. 1-14.

[73] V. *supra*, § 2.

[74] In tale ottica si è, peraltro, anche espresso l'European Data Protection Supervisor, nel bollettino tecnologico "*Neurodata*", 2024, n. 1.

dati devono essere considerati *sempre e comunque* dati non solo *personali*, ma altresì *sensibili*.

Non agevole, infatti, è – lo si è visto poc'anzi – la collocazione dei neurodati in parola nell'ambito delle categorie di dati "speciali" attualmente contemplate dall'art. 9, GDPR.

Va, inoltre, ricordato che la *Raccomandazione* dell'Unesco richiede che i trattamenti dei neurodati siano sottoposti, salvo limitatissime eccezioni, alla regola del consenso informato secondo specifico il modello dell'"*opt-in*"[75].

Da questo punto di vista, non si può non osservare come l'art. 9, GDPR, in materia di dati "sensibili", introduca non ridotte *eccezioni* alla regola del consenso informato. Eccezioni, queste ultime[76], che, per la loro latitudine, potrebbero anche *non* risultare perfettamente in linea col quadro definito dall'Unesco[77].

Una modifica degli articoli 4 e 9 del regolamento (UE) n. 2016/679 che si limitasse "soltanto" alla previsione della "nuova" categoria di neurodati quali dati "sensibili", lasciando, però, inalterate le fattispecie in cui tali dati, divenuti categoria speciale *ex* art. 9, GDPR, possono essere trattati anche in assenza dell'"*opt-in*" dell'interessato, rischierebbe, quindi, di *non* mettere del tutto "in asse" il quadro in materia di protezione dei neurodati europeo rispetto ai principi cardine individuati nella *Raccomandazione* dell'Unesco.

Quanto, poi, ai profili legati alla tutela della salute e della sicurezza d'uso, si può ritenere che alle neurotecnologie sia applicabile la normativa europea sui dispositivi medici di cui al regolamento (UE) n. 2017/745 (MDR)[78].

---

[75] V. *supra*, § 2.

[76] Vale la pena segnalare che nell'ultima *proposta di modifica* di atti regolamentari europei, approvata dalla Commissione europea lo scorso 19 novembre 2025 [COM(2025) 837, "*Digital Omnibus*"], sarebbe prevista l'aggiunta, all'art. 9, par. 2, GDPR, di ulteriori clausole di "esclusione" del divieto di trattamenti di dati c.d. "sensibili" *in assenza* del consenso dell'interessato, fra le quali il trattamento di dati biometrici necessario ai fini della conferma dell'identità dell'interessato se tali dati, o i mezzi necessari alla verifica, sono sotto il controllo esclusivo dell'interessato.

[77] V. *supra*, § 2.

[78] Cfr., per l'analisi della disciplina regolamentare europea, A. Pisani Tedesco, *Dispositivi medici e nuove regole: grandi riforme e qualche occasione persa*, in *Diritto e Salute*, 2022, 3, pp. 19-39; F.G. Cuttaia, *La nuova normativa europea sui dispositivi*

Ai sensi dell'art. 1, MDR, infatti, la disciplina regolamentare concerne l'immissione sul mercato o la messa in servizio, nel territorio dell'Unione, di "dispositivi medici", definiti, ai sensi dell'art. 2, par. 1, n. 1), MDR in termini di «strumento, apparecchio o apparecchiatura o impianto, ivi compreso il *software*, destinato dal fabbricante ad essere impiegato sull'uomo per una […] destinazione d'uso medica» a sua volta consistente nel trattamento di una patologia o di una disabilità, oppure nell'effettuazione di un'indagine, di una sostituzione o di una modificazione di un elemento anatomico o di un processo fisiologico o patologico del corpo umano senza che l'azione principale sia conseguita in via farmacologica, immunologica o metabolica.

Difficile è, dunque, revocare in dubbio che i neuro-dispositivi, impiegati in *contesti sanitari* per *finalità d'uso medico*, ricadano nella definizione di dispositivi medici di cui al regolamento (UE) n. 2017/745 con conseguente applicazione, nei loro confronti, delle norme regolamentari previste.

Lo stesso regolamento (UE) n. 2017/745, all'art. 1, par. 2, in combinato disposto con l'art. 9, estende, peraltro, il proprio raggio di operatività *anche ad alcuni altri tipi dispositivi non aventi uso medicale* indicati puntualmente nell'allegato XVI.

Fra tali dispositivi, al num. 6), rientrano proprio le «[a]ttrezzature destinate alla stimolazione cerebrale che applicano correnti elettriche o campi magnetici o elettromagnetici che attraversano il cranio per modificare l'attività neuronale del cervello». Fattispecie, questa, invero pressoché unica, in cui la vigente disciplina europea pare mettere a fuoco, con un'apposita norma ad essa dedicata, una

---

*medici: una armonizzazione totalmente assorbente delle prerogative legislative degli Stati membri*, in *Rass. dir. farm. salute*, 2017, 5, pp. 940-946; M. Contardi, *Changes in the Medical Device's Regulatory Framework and Its Impact on the Medical Device's Industry: From the Medical Device Directives to the Medical Device Regulations*, in *Erasmus L. Rev.*, 2019, 12(2), pp. 166-177; A. Migliore, *On the New Regulation of Medical Devices*, in *Expert Rev. Med. Devices*, 2017, pp. 921-923; T. Vergani, M. Barrios, F. Carlos, *Needs, Challenges, and Obstacles in the Implementation of the EU Medical Device Regulation*, in *Int. In-House Couns. J.*, 2023, 16(63), pp. 8445-8454; A. Migliore, *On the new regulation of medical devices in Europe*, in *Expert Rev. Med. Devices*, 2017, 14(12), pp. 921-923.

tipologia puntuale di neurotecnologia (nella specie, quella di stimolazione elettro-magnetica trans-cranica[79]).

Ne consegue che sono sottoposti alla disciplina del regolamento (UE) n. 2016/745, i neuro-dispositivi di *qualunque tipo* che *abbiano destinazione d'uso medicale* (art. 2) e altresì i *neuro-dispositivi di stimolazione cerebrale trans-cranica ad onde elettriche o magnetiche non aventi destinazione d'uso medicale* [art. 9 e allegato XVI, num. 6)].

Alla luce di tale disciplina regolamentare, tutti i fabbricanti di *neuro-dispositivi* sono assoggettati agli obblighi di tutela della salute e sicurezza d'uso, stabiliti dagli articoli 10 e seguenti del regolamento (UE) n. 2016/745, i quali comprendono, tra l'altro, l'adozione di un sistema di gestione della qualità e di un sistema di gestione del rischio. Non solo, a norma dell'articolo 5 dello stesso regolamento, il *neuro-dispositivo medico*, alla pari di ogni *altro dispositivo medico*, deve soddisfare i *requisiti generali di sicurezza e prestazione d'uso* stabiliti nell'allegato I in relazione alle proprie caratteristiche. Occorre, poi, sottolineare che i *neuro-dispositivi medici* si collocano, tutti, nelle classi di rischio medio-basso, medio-alto e alto – classi IIa, IIb e III – di cui all'articolo 51 e all'allegato VIII[80].

Infatti, i neuro-dispositivi medici che vengano a *contatto diretto con il sistema nervoso centrale* (come gli impianti cerebrali) devono essere classificati come dispositivi medici di classe III (ad alto rischio) secondo la regola 8, 2° trattino, allegato VIII, MDR.

---

[79] Si tratta, giova sottolinearlo, di una tecnologia che può essere impiegata anche a fini di "potenziamento" cognitivo-sensoriale umano. Vi è, in effetti, chi ritiene possibile che, in un *non* troppo remoto futuro, si giunga anche ad una sorta di "potenziamento" non solo delle funzioni cerebrali legate all'elaborazione degli stimoli sensoriali o dei processi di memoria e ragionamento, ma altresì delle stesse abilità di giudizio "morale". Cfr., per il dibattito in parola, I. PERSON, J. SAVULESCU, *Inadatti al futuro. L'esigenza di un potenziamento morale*, Torino, 2019; J. HARRIS, *How to be Good: The Possibility of Moral Enhancement*, Oxford, 2018; P.S. CHURCHLAND, *Neurobiologia della morale*, Milano, 2012.

[80] In punto, preziosa è la ricostruzione della trama di regole europee applicabili ai neuro-apparecchi quali dispositivi medici e non medici (questi ultimi, in quanto dispositivi di stimolazione trans-cranica del cervello) svolta da C. BUBLITZ, S. LIGTHART, *The new regulation of non-medical neurotechnologies in the European Union: overview and reflection*, in *J.L. & Biosciences*, 2024, pp. 8-9.

I neuro-dispositivi medici che, pur *non* entrando in contatto diretto con il tessuto cerebrale, sono comunque *invasivi* (come un dispositivo per risonanza magnetica), si collocano parimenti in classe III in quanto si tratta di apparecchi dipendenti, nel loro funzionamento, dall'energia elettrica (e quindi "*attivi*", *ex* art. 2, n. 4), MDR), secondo la regola 8, 6° trattino, allegato VIII, MDR.

I neuro-dispositivi medici *non invasivi* (come un "caschetto" a onde cerebrali) ricadono, a loro volta, nella classe IIa (a rischio medio-basso) in quanto utilizzano energia destinata ad essere assorbita dal corpo umano secondo la regola 10, allegato VIII, MDR, fatto salvo il loro collocamento in classe IIb (a rischio medio-alto), qualora siano destinati al monitoraggio di parametri fisiologici vitali del sistema nervoso centrale e la natura delle variazioni di tali parametri sia tale da poter comportare un pericolo immediato per il paziente o il paziente medesimo versi in una condizione clinica di pericolo imminente in base alla regola 10, allegato VIII, MDR.

Sono analogamente inseriti in classe IIb i neuro-dispositivi che *analizzino* il sistema nervoso del paziente mediante l'emissione di *radiazioni ionizzanti* (quali, ad esempio, la comune tomografia assiale computerizzata) secondo quanto stabilito dalla regola 10, allegato VIII, MDR.

I neuro-dispositivi medici di *stimolazione dell'attività neuronale* (come gli apparecchi trans-cranici elettromagnetici) sono, poi, assoggettati alla stessa classe IIb in quanto operano somministrando energia (sono "attivi") all'interno del corpo umano in modo "potenzialmente pericoloso" a causa del "sito di applicazione dell'energia" che, nel caso di specie, è il cervello, secondo la regola 9, allegato VIII, MDR.

Infine, i *neuro-dispositivi medici* che regolino in modo bidirezionale la propria attività in risposta alle reazioni neuronali (c.d. dispositivi "*closed loop*") sono classificati in classe III (ad alto rischio) sulla base della regola 22, allegato VIII, MDR.

Nei confronti di *tutti* i neuro-dispositivi *medici* saranno, quindi, valevoli le regole "rafforzate" in punto tutela della sicurezza e della salute dettate per le classi IIa, IIb e III (rischio medio-basso, medio-alto ed elevato) del regolamento (UE) n. 2016/745.

I neuro-dispositivi *non medici*, di cui all'allegato XVI, n. 6), MDR, sono, a loro volta, collocati, in forza di quanto nei loro riguardi direttamente dispone il regolamento d'esecuzione (UE) n. 2022/2347, nella classe III, MDR (quella a rischio più elevato) con conseguente obbligo, per il produttore, non solo di condurre indagini cliniche prima della loro commercializzazione, ma altresì di seguire le apposite, e assai dettagliate, misure di gestione del rischio fissate, per questa (*sola*) *tipologia di neuro-dispositivi*, dal regolamento d'esecuzione (UE) n. 2022/2346.

Si tratta, in specifico, dell'obbligo di condurre puntuali valutazioni sugli effetti di ordine psicologico che l'uso dei neuro-stimolatori elettro-magnetici può implicare, nonché sulle variazioni, relativamente alla conformazione e all'attività cerebrale, che possono essere indotte dal ricorso alla neuro-stimolazione trans-cranica.

È, inoltre, richiesto ai produttori di neurodispositivi di stimolazione cerebrale trans-cranica di introdurre, "*by design*", meccanismi automatizzati volti a limitare oltre una certa soglia di potenza o durata d'impiego l'emissione degli impulsi potenzianti.

È, infine, fatto divieto di commercializzare i neuro-dispositivi di stimolazione in parola a persone affette da epilessia o sottoposte a trattamenti con psicofarmaci; a malati di tumore o ai soggetti colpiti da altre patologie cerebrali; a minori e donne in stato di gravidanza salvo che vengano fornite prove incontrovertibili che dimostrino l'assoluta sicurezza d'uso.

Il quadro di regole volte ad assicurare la tutela del diritto all'integrità psico-fisica ed alla salute di cui al regolamento (UE) n. 2017/745, *non* trova, invece, applicazione rispetto a tutti gli altri tipi di *neuro-dispositivi non aventi destinazione d'uso medica* e altresì *diversi dai neuro-stimolatori a onde elettromagnetiche*.

Per tutte queste tipologie di neuro-dispositivi, perciò, il *diritto alla salute e all'integrità psico-fisica* dell'utilizzatore umano, sarà tutelato soltanto in base alla disciplina generale dettata per la *sicurezza dei prodotti in commercio* dal regolamento (UE) n. 2023/988[81], la

[81] Sul punto, in generale, cfr. E. STEINDL, *Consumer neuro devices within EU products safety law: Are we prepared for big tech ante portas?*, in *Comput. L. & Sec. Rev.*, 2024, 52, pp. 1-9.

quale contempla, comunque, lo svolgimento obbligatorio (almeno) di *valutazioni di impatto* legate al *rischio per la salute e la sicurezza* associato all'uso del prodotto (nella specie, del prodotto "*neuro-tecnologico*").

L'ordinamento dell'Unione europea, quindi, pur assicurando una robusta tutela dei diritti alla salute e all'integrità psico-fisica delle persone che si servono di neuro-dispositivi in ambito medico, e pur contemplando una disciplina particolarmente rigorosa per i dispositivi di elettro-stimolazione cerebrale *non* utilizzati in campo sanitario, risulta imperfettamente "calibrato" rispetto alle previsioni della *Raccomandazione* dell'UNESCO per quanto attiene a tutti gli altri neuro-dispositivi. Questi ultimi, infatti, sono disciplinati dalle regole dettate per la sicurezza dei prodotti in generale, che risultano meno robuste, in punto tutela dell'integrità psico-fisica e degli altri diritti fondamentali, rispetto a quanto la Raccomandazione indica sia necessario per apparecchiature neuro-tecnologiche destinate all'uso commerciale diffuso in ragione della influenza, che tali macchinari possono avere, su fattori di elevata delicatezza quali sono i meccanismi di funzionamento del cervello[82].

Emerge, quindi, un potenziale elemento di "debolezza" nella piena tutela dei diritti della persona assicurata dall'ordinamento dell'Unione europea rispetto a neuro-tecnologie destinate a un promettente mercato di consumatori e per le quali la *Raccomandazione* dell'Unesco auspica, da parte degli Stati, l'introduzione di regole specifiche.

Infine, pur *non* facendovi esplicito riferimento[83], può trovare applicazione *anche* alle neurotecnologie e al trattamento dei neuro-

[82] V. *supra*, § 2.

[83] Giova osservare che l'unico riferimento esplicito a un "neuro-dispositivo" contenuto nel regolamento (UE) n. 2024/1689, è rilevabile al considerando n. 97) con riferimento alle tecniche di manipolazione basate sull'uso di intelligenza artificiale che risultano vietate in quanto utilizzate per persuadere le persone ad adottare comportamenti indesiderati oppure per indurle, con l'inganno e anche attraverso mezzi subliminali, a prendere decisioni in modo tale da sovvertirne e pregiudicarne l'autonomia, o il processo decisionale o la libera scelta, oppure in modo da patire effetti negativi sufficientemente importanti sulla propria salute fisica, psicologica o sugli interessi finanziari. Si tratta infatti – come sottolinea lo stesso considerando n. 97) – di tecniche, quelle qui menzionate, che ben potrebbero essere facilitate «ad esempio, da interfacce

dati, il regolamento (UE) n. 2024/1689 (AIA) in materia di *intelligenza artificiale*[84].

Infatti, tutti quei dispositivi neurotecnologici che richiedono, per poter svolgere in modo adeguato la loro funzione, l'elaborazione di una grande quantità di dati e lo sviluppo di una significativa capacità di autoapprendimento a partire dai segnali neuronali specifici dell'individuo che li usa – come accade con le interfacce cervello-computer o con i dispositivi "closed-loop" – richiedono di servirsi di sistemi di intelligenza artificiale secondo la definizione che di questi ultimi è data dall'art. 3, par. 1, n. 1), AIA[85].

L'applicazione anche ai "*neuro-dispositivi muniti di IA*" della disciplina di cui al regolamento (UE) n. 2024/1689 introduce, dunque, un ulteriore *livello di protezione dei neuro-diritti* in Europa oltre a quello assicurato dal regolamento (UE) n. 2016/679 e dal regolamento (UE) n. 2017/745, sin qui accennati, nonché dal regolamento (UE) n. 2023/988 per i neuro-prodotti commerciabili in generale.

---

cervello-computer o dalla realtà virtuale, in quanto queste consentono un livello più elevato di controllo degli stimoli presentati alle persone, nella misura in cui possono distorcerne materialmente il comportamento in modo significativamente nocivo».

Un riferimento parimenti esplicito, e più ampio, alle neurotecnologie è rinvenibile, recentemente, nella comunicazione della Commissione relativa agli *Orientamenti della Commissione relativi alle pratiche di intelligenza artificiale vietate ai sensi del regolamento (UE) 2024/1689 (regolamento sull'IA)* [C(2025) 5052 final] del 29 luglio 2025 ove si puntualizza, al n. 66), che con il rapido sviluppo, fra le altre, delle neurotecnologie e delle interfacce cervello-computer si elevano i rischi di manipolazione subdola e sofisticata del comportamento umano grazie alla possibilità di agire a livello subconscio mediante pratiche di "*dream-hacking*" e "*brain spyware*" servendosi di neuro-dispositivi che, creduti dall'utente utilizzati solamente per controllare un semplice videogioco, sono, in realtà, anche in grado di indurre il cervello dell'utente, in modo surrettizio e senza che questi ne sia consapevole, a rivelare informazioni che potrebbero essere altamente sensibili.

[84] Cfr., per tutti, l'approfondita disamina, con riflessioni particolarmente feconde, condotta da M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, in F. Pizzetti, S. Calzolaio, A. Iannucci, E. Longo, M. Orofino, *La regolazione europea dell'intelligenza artificiale nella società digitale*, Torino, 2025, pp. 33-62.

[85] Cfr. U. Ruffo, M. Gabrielli (a cura di), *Intelligenza Artificiale, dispositivi medici e diritto. Un dialogo fra saperi: giuristi, medici e informatici a confronto*, Torino, Giappichelli, 2023; M. Ienca, K. Ignatiadis, *Artificial intelligence in clinical neuroscience: methodological and ethical challenges*, in *AJOB Neuroscience*, 2020, 11(2), pp. 77-87.

Innanzitutto, infatti, sarà *vietato*, sull'intero territorio dell'Unione europea, il ricorso a *neuro-dispositivi con IA che presentano rischi ritenuti "inaccettabili"* in base all'art. 5, AIA.

Si tratta, in particolare, di tutti quei neuro-dispositivi, *dotati di sistemi di intelligenza artificiale*, che permettono *tecniche di manipolazione subliminale o ingannevoli* mediante l'accesso, la registrazione o l'alterazione dei segnali cerebrali, oppure che *sfruttano vulnerabilità derivanti dall'età o dalla disabilità* facendo leva sulle componenti cerebrali della fragilità, oppure ancora che *valutano le persone sulla base di comportamenti sociali o caratteristiche personali* derivanti da fattori neurologici al fine di assegnare loro un "*punteggio sociale*" (c.d. "*social scoring*"), o che si servono di dati biometrici ricavati dal cervello per giungere a *categorizzare gli individui* in ragione di elementi sensibili o che, infine, permettono, attraverso l'acquisizione e l'elaborazione di dati cerebrali, il *riconoscimento delle emozioni in ambito lavorativo e scolastico* (salvo che ricorrano specifiche e preminenti ragioni di salute e sicurezza).

Tutti usi, questi, rispetto ai quali la Raccomandazione dell'Unesco fissa (come si è visto)[86] appositi "paletti" a tutela della dignità e dell'autodeterminazione, nonché degli altri diritti fondamentali della persona.

In secondo luogo, saranno sottoposti alla *rigorosa disciplina* prevista per i sistemi di IA "*ad alto rischio*", di cui al medesimo regolamento (UE) n. 2024/1689, tutti quei *neuro-dispositivi muniti di IA* che ricadono nelle normative di armonizzazione dell'Unione europea elencate nell'allegato I e che richiedono la valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio secondo quanto stabilito dall'art. 6, par. 1, AIA.

Si tratta di normative europee di armonizzazione fra le quali è incluso, al num. 11) della sezione A), anche il regolamento (UE) n. 2017/745 sui dispositivi medici.

Di conseguenza, *un sistema di IA* destinato a essere utilizzato come componente di un *dispositivo medico sottoposto a una valutazione della conformità da parte di terzi* ai fini dell'immissione sul

[86] V. *supra*, § 2.

mercato o della messa in servizio sarà sempre considerato "ad alto rischio" in base all'art. 6, par. 1, e all'allegato I, sez. A), num. 11), AIA.

Ora, dal momento che, ai sensi del regolamento (UE) n. 2017/745, i *dispositivi medici* riconducibili alle classi di rischio IIa, IIb e III prevedono *tutti* l'*intervento dell'organismo notificato* ai fini della verifica di conformità del prodotto propedeutica all'immissione in commercio, *tutti* i *neuro-dispositivi medici* che siano anche *muniti di IA* saranno anche regolati dalla disciplina prevista dal regolamento (UE) n. 2024/1689 per i sistemi di IA "ad alto rischio"[87].

Non solo. Saranno sottoposti alle stesse norme anche i *neuro-dispositivi non medici ma di potenziamento cerebrale* che siano parimenti *muniti di IA.*

Tali dispositivi, infatti, ricadono nella classe III ai sensi dell'allegato XVI, n. 6, MDR e del regolamento d'esecuzione (UE) n. 2022/2347. E poiché nei loro confronti, proprio in quanto apparecchi medici di classe III, è sempre d'obbligo la valutazione di conformità da parte dell'organismo notificato prima della messa in commercio, anche questi tipi di neuro-apparecchi devono essere rite-

[87] Il documento "*Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)*", adottato congiuntamente dall'Artificial Intelligence Board e dal Medical Device Coordination Group, n. AIB 2025-1/MDCG 2025-6, colloca le discipline di cui al regolamento (UE) n. 2024/1689 e al regolamento n. 2017/745 in un rapporto di reciproca *complementarietà* con il conseguente riconoscimento, a favore dei produttori di dispositivi medici integrati da sistemi di IA (MDAI), della clausola di flessibilità di cui all'art. 8, par. 2, del regolamento (UE) n. 2024/1689.

Sui rapporti fra la disciplina sui dispositivi medici e la normazione in materia di sistemi di intelligenza artificiale, può essere utile il contributo di V. Di Capua, *AI and Disease Diagnosis: Legal Aspects*, in *Corti Supreme e salute*, 2024, 1, pp. 344-363.

In proposito, merita di segnalare che la Commissione europea ha presentato, il 19 novembre 2025, una *proposta* di modifica del regolamento (UE) n. 2024/1689 [COM(2025) 836, "*Digital Omnibus on AI*", che, laddove venisse in futuro approvata, prevede il ricorso ad un'unica procedura di valutazione della conformità in base a una sola istanza nel caso di prodotti contenenti sistemi di IA già soggetti a normativa di armonizzazione ai sensi dell'all. I, sez. A, AIA fra i quali vengono espressamente contemplati proprio i dispositivi medici di cui al regolamento (UE) n. 2017/745 [cfr. considerando n. 7) della proposta]. Va, peraltro, evidenziato che la *proposta*, se varata, contemplerebbe anche il differimento temporale dell'applicazione della disciplina prevista per i sistemi di IA "ad alto rischio" (ivi compresi, quindi, quelli in questa sede considerati) rispetto alla data attualmente fissata per il 2 agosto 2026.

nuti, ai sensi dell'art. 6, par. 1 e dell'allegato I, sez. A) num. 11), AIA, sistemi di intelligenza artificiale "ad alto rischio".

Tutti i neuro-dispositivi *medici* e quelli *non medici* di stimolazione elettromagnetica cerebrale muniti di IA (c.d. "MDAI") saranno, perciò, usufruibili sul mercato europeo soltanto dopo essere stati sottoposti a una valutazione di conformità che ne attesti il pieno rispetto dei requisiti – piuttosto stringenti – previsti dalla normativa regolamentare per l'IA "rischiosa".

Non basta. L'art. 6, par. 2 del regolamento (UE) n. 2024/1689 stabilisce, infatti, che siano considerati "ad alto rischio", anche i sistemi di IA riconducibili ai contenuti dell'allegato III, AIA[88]. Si tratta di sistemi che operano, con talune modalità e finalità specificamente enumerate, nel campo della biometria, dell'istruzione e formazione professionale, del lavoro, dei servizi pubblici (e privati) essenziali, dell'immigrazione, del contrasto alla criminalità e della giustizia.

Rientreranno, quindi, fra i *neuro-dispositivi muniti di IA "ad alto rischio"*, ai sensi dell'art. 6, par. 2 e dell'allegato III, del regolamento (UE) n. 2024/1689, anche quelli che vengono impiegati per il *riconoscimento e la categorizzazione biometrica o emozionale* sulla base di "*pattern* cerebrali" [all. III, num. 1)], oppure per la *valutazione dei rendimenti in ambito scolastico e lavorativo* mediante la captazione e l'analisi dei fattori cerebrali durante l'attività di apprendimento o di lavoro [all. III, num. 3) e all. III, num. 4)], oppure per l'*analisi probabilistica sulla recidiva del reo* in campo giudiziario (intercettando, per dire, eventuali anomalie anatomico-funzionali in aree del cervello che potrebbero diminuire l'efficacia dei "freni inibitori") [all. III, num. 8)], oppure per la valutazione, sulla base di indagini mediche relative a patologie neurologiche, dell'affidabilità

[88] Per completezza, si segnala che, in base all'art. 6, paragrafi da 3 a 8, AIA, *non* è considerato ad alto rischio un sistema di cui all'allegato III se esso *non* presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche anche nel senso di *non* influenzare materialmente il risultato del processo decisionale (ad esempio perché il sistema di IA è destinato a eseguire un compito limitato dal punto di vista procedurale, oppure perché il sistema di IA è destinato a migliorare il risultato di un'attività umana che si è già precedentemente completata, oppure ancora perché il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti senza sostituire o influenzare la valutazione umana).

creditizia o della maggior alea della persona fisica che intende accendere un mutuo, effettuare un investimento, o stipulare un'assicurazione sanitaria o sulla vita [all. III, num. 5)]. Tutti contesti, questi ultimi, rispetto ai quali non mancano nella *Raccomandazione* dell'Unesco – come si è visto[89] – previsioni assai stringenti per la protezione dei diritti della persona dal ricorso alle neurotecnologie.

Anche a tali "neuro-dispositivi" che incorporano sistemi di IA considerati "ad alto rischio" si applicheranno, di conseguenza, le molteplici previsioni, di cui al Capo III del regolamento (UE) n. 2024/1689, relative ai sistemi di IA "ad alto rischio" in generale e che riguardano, oltre agli organismi notificati preposti alla verifica di conformità e all'adozione di meccanismi di assicurazione della qualità da parte dei produttori, anche i requisiti che i sistemi stessi devono rispettare; i sistemi di gestione del rischio che essi devono implementare; la *governance* dei dati trattati che debbono assicurare [la quale si affianca alle disposizioni del regolamento (UE) n. 2016/679[90] con particolare attenzione a quelli utilizzati per l'addestramento o la prova del sistema[91]]; la documentazione tecnica di riferimento di cui devono essere corredati; le attività oggetto di monitoraggio che vanno condotte durante il loro impiego; la supervisione umana che deve essere garantita mentre sono in funzione; l'accuratezza, robustezza e cyber-sicurezza coi quali essi devono essere fabbricati.

---

[89] V. *supra*, § 2.

[90] Prevede, infatti, testualmente, l'art. 2, par. 7, AIA che resta impregiudicato il regolamento (UE) 2016/679 nel quadro del diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni.

[91] Assume significativo rilievo, in relazione alla peculiare natura dei dati cerebrali quali dati c.d. "sensibili", la previsione, di cui all'art. 10 AIA, relativamente ai data-set di prova e di addestramento dei sistemi di IA "ad alto rischio" in generale che, applicata ai "neuro-dispositivi" dotati di IA, consente ai fornitori, limitatamente allo scopo di garantire il rilevamento e la correzione delle distorsioni ("*bias*") del sistema, di trattare anche neuro-dati nei limiti di quanto stabilito dal regolamento (UE) n. 2016/679 e purché il rilevamento e la correzione delle distorsioni non possano essere efficacemente conseguiti mediante il trattamento di altri dati, ivi compresi quelli sintetici o anonimizzati; venga privilegiata la pseudonimizzazione nel quadro delle limitazioni ai trattamenti funzionali alla salvaguardia della vita privata; siano implementate avanzate misure tecniche di sicurezza in modo da escludere che le persone non autorizzate abbiano accesso ai dati in questione.

Si osservi, inoltre, che ai sensi dell'art. 27 del regolamento (UE) n. 2024/1689, i *deployer* organismi di diritto pubblico o enti privati che forniscono servizi pubblici e i *deployer* che forniscono sistemi di IA ad alto rischio, di cui all'allegato III, punto 5, lettere *b*) e *c*) (si tratta della valutazione di merito creditizio o di alea assicurativa), sono tenuti a effettuare, prima di utilizzare un sistema di IA ad alto rischio[92], un'apposita "*valutazione dell'impatto sui diritti fondamentali*" (FRIA)[93].

Si tratta di una valutazione consistente – in estrema sintesi – nel descrivere, da parte del *deployer*, i processi pertinenti in cui il sistema di IA sarà impiegato (con indicazione anche del periodo di tempo e della frequenza d'uso), nonché nell'individuare le categorie specifiche di persone e di gruppi interessati e nel fornire, altresì, la dettagliata elencazione di rischi specifici di danno per i diritti fondamentali che possono verificarsi dall'uso del dispositivo prevedendo le misure da adottare al verificarsi dell'evento per mitigarne gli effetti, ivi compreso il ricorso alla sorveglianza umana.

Tale valutazione di impatto sui diritti fondamentali (FRIA), la quale si accompagna alla *valutazione di impatto sulla protezione dei dati* (DPIA), prevista dall'art. 35, GDPR, è particolarmente significativa giacché essa appare consonante all'omonimo strumento indicato nella *Raccomandazione* dell'Unesco per prevenire o mitigare possibili effetti lesivi sui diritti fondamentali (e sulla violazione della *privacy*) derivanti dall'uso delle neurotecnologie[94].

In base al regolamento (UE) n. 2024/1689, l'obbligo per il *deployer* di condurre la valutazione di impatto sui diritti fondamentali sussiste, però, *solo* nel caso in cui il *deployer* stesso sia un organismo pubblico, oppure un soggetto privato fornitore di servizi pubblici e il sistema di IA sia "ad alto rischio" ai sensi dell'art. 6, par. 1, o

---

[92] Secondo l'art. 6, par. 2, AIA, *esclusi* i sistemi destinati ad essere usati nel settore di cui all'allegato III, punto 2, AIA.

[93] Cfr., in particolare, A. Mantelero, *The Fundamental Rights Impact Assessment (FRIA) In the AI Act: Roots, legal obligation and key elements for a model template*, in *Comput. L. & Sec. Rev.*, 2024, 54, pp. 1-18; H. Janssen, M. Seng Ah Lee, J. Singh, *Practical fundamental rights impact assessments*, in *Int. J. Law Inf. Technol.*, 2022, 30(2), pp. 200-232.

[94] V. *supra*, § 2.

dell'art. 6, par. 2, allegato III AIA, limitatamente al punto 5), lett. *b*) e *c*).

Ai fini della sussistenza dell'obbligo di espletare la FRIA, occorre, quindi, che il neuro-dispositivo munito di IA utilizzato dal *deployer* sia un *neuro-dispositivo medico* o un *neuro-dispositivo non medico di stimolazione cerebrale* giacché è in tali casi che si è in presenza di un sistema di IA ad alto rischio secondo l'art. 6, par. 1, AIA sottoposto anche alla FRIA a norma dell'art. 27, AIA; oppure, si deve trattare di un *neuro-dispositivo* contenente IA impiegato dal *deployer* per la valutazione del merito creditizio o dell'alea assicurativa visto che è in tali casi che si sarà in presenza di un sistema di IA ad alto rischio secondo l'art. 6, par. 2, AIA, oggetto anche alla FRIA a norma dell'art. 27, AIA.

Da una parte, quindi, il regolamento (UE) n. 2024/1689 prevede misure assai stringenti per assicurare il rispetto della dignità umana e dei diritti fondamentali della persona, inclusa un'apposita valutazione di impatto sui diritti fondamentali in relazione ai rischi potenzialmente insiti nell'impiego dei neuro-dispositivi.

Dall'altra parte, però, tali cogenti e protettive misure risultano applicabili *non* già in ragione della caratteristica "neuro-tecnologica" del dispositivo, bensì *solo* in quanto lo stesso neuro-dispositivo (come un qualunque altro apparecchio di tipo diverso) incorpori un sistema di IA ad alto o inaccettabile rischio.

Il che significa che *non* tutti i neuro-dispositivi per i quali la *Raccomandazione* dell'Unesco richiede agli Stati di adottare un quadro giuridico *robusto* a tutela dei *diritti fondamentali coinvolti*[95], risultano sottoponibili alla disciplina fissata dal regolamento (UE) n. 2024/1689.

Non *tutti* i neuro-dispositivi incorporano, infatti, nel loro ordinario funzionamento sistemi di IA[96].

Senza contare che anche nel caso in cui vengano in rilievo le regole europee sull'intelligenza artificiale, il neuro-dispositivo potrebbe *non* esser considerato comunque "ad alto rischio" o "a rischio inaccettabile" dato che la disciplina, di cui al regolamento

[95] V. *supra*, § 2.
[96] V. *supra*, § 3.

(UE) n. 2024/1689, individua i livelli di rischio indipendentemente dalla caratteristica che il sistema di IA interagisca col cervello umano.

Potrebbero, quindi, essere immessi sul mercato anche neuro-dispositivi che, dal punto di vista della loro *dotazione di sistemi di intelligenza artificiale*, *non* presentano profili di rischio tali da giustificare le misure di protezione previste dal regolamento (UE) n. 2024/1689 ma che, nondimeno, per loro *potenzialità di interazione col cervello umano*, assumono un fattore di *elevata pericolosità* che richiederebbe, alla luce della *Raccomandazione* dell'Unesco, l'adozione di apposite *misure protettive della persona* in relazione ai suoi *diritti fondamentali*[97].

Anche la valutazione di impatto sui diritti fondamentali – che, insieme alla valutazione di impatto sulla protezione dei dati, costituisce elemento qualificante della strategia europea di tutela dei diritti della persona nella società digitale e che è altresì contemplata dalla *Raccomandazione* dell'Unesco quale strumento rilevante per la protezione dei diritti individuali rispetto all'uso delle neurotecnologie[98] – *non* è richiesta per tutti i neuro-dispositivi dotati di intelligenza artificiale, *né*, tanto meno, è obbligatoria per i neuro-apparecchi che siano *privi* di IA nonostante l'incidenza che l'uso di tali aggeggi può avere per i diritti del soggetto[99], soprattutto in quei settori che la stessa *Raccomandazione* considera meritevoli di tutele apposite e rafforzate a piena salvaguardia dei diritti dei soggetti (anche fragili) coinvolti.

## 4. *Considerazioni conclusive*

Dall'analisi sin qui compiuta, pare, allora, di potersi ritenere che l'Unione europea, forte dei valori e dei diritti fondamentali da essa stessa sanciti a livello di diritto primario e pienamente consonanti coi princìpi in corso di elaborazione a livello di diritto internazionale sulle neurotecnologie, potrà essere chiamata, nel prossimo futuro, a compiere alcuni passi di "adattamento" del proprio

[97] V. *supra*, § 3.
[98] V. *supra*, § 2.
[99] V. *supra*, § 3.

diritto derivato allo scopo di mettersi "pienamente in asse" con l'orizzonte di salvaguardia e promozione dei neurodiritti emergente dalla *Raccomandazione* dell'Unesco recentissimamente adottata.

La vigente regolazione europea di diritto derivato, infatti, riguardante (anche) i neuro-dispositivi e i neurodati – frutto dell'intersecarsi, in un complesso prisma dalle molteplici facce, di discipline differenti (nessuna, invero, appositamente costruita con riferimento alla neurotecnologia che è, nel suo genere, unica) – rischia non solo di comportare una continua e paziente opera di tessitura fra norme diverse, la quale può generare difficoltà e incertezze interpretative e applicative con conseguenti ostacoli alla produzione e all'uso di neuro-dispositivi in Europa, ma anche di *non* assicurare *appieno* l'aderenza del Vecchio Continente ai più recenti e avanzati sviluppi normativi per la protezione della dignità e dei diritti fondamentali emersi a livello internazionale in relazione ai neuro-dispositivi e al trattamento dei neurodati.

Da una parte, infatti, il regolamento (UE) n. 2016/679, in materia di *diritto alla protezione dei dati cerebrali*, non menziona espressamente i neurodati fra le categorie di dati "sensibili" al contrario di quanto la *Raccomandazione* dell'Unesco sollecita gli Stati a fare[100], né prescrive, per i trattamenti di tali dati, che la regola del consenso informato dell'interessato non subisca (salvo che rarissime) eccezioni[101]; nemmeno il regolamento in parola individua tutele rafforzate in relazione ai trattamenti di dati neuronali nei contesti maggiormente "delicati" di impiego delle neuro-tecnologie[102] ai quali, invece, la *Raccomandazione* fa esplicito riferimento (dall'istruzione e formazione, al lavoro)[103].

Da un'altra parte, il regolamento (UE) n. 2017/745, pur offrendo un solido quadro di tutela del *diritto alla salute e all'integrità psico-fisica* rispetto ai neuro-dispositivi per *uso clinico* e ai neuro-dispositivi *non* per *uso clinico* di *stimolazione cerebrale trans-cranica*, *non* si estende anche agli *altri e diversi tipi di neuro-dispositivi*, sem-

[100] V. *supra*, § 2.
[101] V. *supra*, § 3.
[102] V. *supra*, § 3.
[103] V. *supra*, § 2.

pre più numerosi e diffusi[104] rispetto ai quali la *Raccomandazione* dedica peculiare attenzione in punto tutela della salute e della sicurezza d'uso[105].

Da un'altra parte, ancora, se la tutela degli *altri diritti fondamentali* della persona – diversi dalla protezione dati e della *salute* – rispetto ai neuro-dispositivi *muniti di IA* pare essere assicurata, anche mediante il ricorso ad apposite "valutazioni di impatto sui diritti fondamentali", dal regolamento (UE) n. 2024/1689[106], non si può non evidenziare come la legislazione in materia di intelligenza artificiale *non* si applichi alle neurotecnologie che *non* contengono al proprio interno *elementi di IA* lasciando, quindi, tali tecnologie prive delle misure contemplate dallo stesso regolamento (UE) n. 2024/1689, anche laddove esse presentino, per le loro peculiari caratteristiche di interagire in vario modo con cervello umano, rischi alti o inaccettabili per la dignità e i diritti fondamentali della persona e richiedano, di conseguenza, secondo la *Raccomandazione dell'Unesco*, una regolazione specifica[107].

Se, com'è stato autorevolmente sottolineato, «il cervello è sempre di più l'ultima frontiera della privacy» giacché esso «può essere infiltrato e monitorato come tutte le nostre telefonate e attività online» mentre gli stessi dati cerebrali possono essere «raccolti e aggregati proprio come quelli dei movimenti finanziari e dello shopping online»[108], un'Unione europea che voglia continuare a salvaguardare appieno i valori su cui si fonda, nel quadro di un rinnovato umanesimo che ponga pienamente "al centro" la dignità della persona umana[109], non può che interrogarsi sulla prospettiva di adottare una *propria*, *apposita*, *regolamentazione*, orientata alla *tutela dei di-*

---

[104] V. *supra*, § 3.

[105] V. *supra*, § 2.

[106] V. *supra*, § 3.

[107] V. *supra*, § 2.

[108] N. Farahany, *Difendere il nostro cervello: La libertà di pensiero nell'era delle neurotecnologie*, Torino, 2024, pp. 19-20.

[109] Secondo l'espressione, particolarmente suggestiva, adoperata dal Presidente della Repubblica Sergio Mattarella, in un discorso tenuto il 25 agosto 2025 al XLIV *Meeeting per l'amicizia fra i popoli*, con riferimento, fra l'altro, proprio alle innovazioni «neuro-scientifiche».

*ritti fondamentali* rispetto alle *neurotecnologie* e ai *neurodati*[110] così come essa, prima nel mondo, ha avuto l'audacia di fare in relazione all'altra "rivoluzione" – quella dell'intelligenza artificiale[111] – che così profondamente e significativamente connota il nostro tempo.

[110] Scegliendo, in particolare, un modello di regolazione che combini armoniosamente l'approccio orientato ai diritti, quello rivolto alle specificità dei contesti di impiego e quello ispirato da rispetto per la scienza (cfr., in generale, G. De Gregorio, P. Dunn, *The European risk-based approaches: connecting constitutional dots in the digital age*, in *C.M.L. Rev.*, 2022, 59(2), pp. 473-500; J. Black, R. Baldwin, *Really responsive risk-based regulation*, in *Law & Pol.*, 2010, 32(2), pp. 181-213; M. Dawson, *The Governance of EU Fundamental Rights*, Cambridge, 2017) senza lasciarsi dominare dalla paura dell'innovazione (freno eccessivo al progresso della persona e della collettività), né trascinare da esacerbate utopie trans-umaniste (che rischiano di essere disumanizzanti: cfr., in punto, A. Carrara (a cura di), *Neurobioetica e transumanismo*, Roma, 2021).

[111] Nell'allocuzione pronunciata il 10 maggio 2025 davanti al Collegio cardinalizio riunito, il neoeletto Papa Leone XIV ha indicato, fra le diverse ragioni che lo hanno orientato nella scelta del nome pontificale, anche quella di volersi espressamente ricollegare alla dottrina sociale della Chiesa, il cui sviluppo è storicamente iniziato con l'enciclica "*Rerum Novarum*" del suo predecessore Papa Leone XIII (1891), nel quadro di una rinnovata risposta che la stessa Chiesa intende, oggi, offrire in relazione a quella che il Pontefice definisce «un'altra rivoluzione industriale e agli sviluppi dell'intelligenza artificiale, che comportano nuove sfide per la difesa della dignità umana, della giustizia e del lavoro».

STEFANIA SERAFINI

# LA CESSIONE DELL'INFRASTRUTTURA DI RETE DI TELECOMUNICAZIONE FISSA: QUESTIONI REGOLATORIE E CONCORRENZIALI



## 1. *La cessione della rete Tim: la vicenda*

La cessione da parte dell'ex monopolista legale della rete infrastrutturale di telecomunicazioni in postazione fissa italiana, oltre a rappresentare un evento cruciale dal punto di vista della valutazione dello sviluppo economico e della crescita industriale del nostro Paese, andando ad incidere in un settore altamente strategico, ha determinato un mutamento radicale – unico nel panorama europeo – nella configurazione del mercato delle comunicazioni elettroniche, che fin dal suo esordio era stato caratterizzato da un'integrazione verticale tra l'impresa detentrice della più importante infrastruttura di rete e l'impresa avente una posizione dominante nel mercato al dettaglio della fornitura dei servizi di trasmissione voce e dati[1].

[1] La ragione della connaturata integrazione verticale tra il detentore della rete e l'impresa in posizione dominante nel mercato dei servizi di telecomunicazione deve farsi risalire alle caratteristiche del mercato, rientrante nei c.d. *servizi a rete*, e rappre-

L'operazione di cessione della rete si è, in vero, posta in modo coerente con la visione accolta nel nuovo Codice Europeo della Comunicazioni Elettroniche, introdotto con la Direttiva UE n. 2018/1972, che è andato nella direzione di superare il modello che aveva accompagnato la liberalizzazione del settore e che si connotava per la promozione di una concorrenza nel solo mercato dei servizi al dettaglio (c.d. *service and access based competition*)[2], da rea-

---

sentate dal fatto che essi necessitano di un'infrastruttura altamente costosa nella sua realizzazione e manutenzione, il che ha fatto sì che nei primi decenni del '900 in tutti i paesi industrializzati la fornitura dei servizi di telecomunicazione nascesse protetta da monopoli legali affidati ad imprese pubbliche. Il percorso che ha portato alla liberalizzazione dei mercati delle telecomunicazioni ha preso le mosse con il Libro Verde della Commissione Europea del 28 novembre 1987, volto ad introdurre una graduale liberalizzazione partendo dai servizi accessori, e lasciando in un primo momento la gestione della rete e del servizio primario di fonia vocale ai gestori pubblici (i.e. in Italia il Ministero delle Poste e delle Telecomunicazioni). Sotto la spinta delle politiche europee, a partire dagli anni Novanta, è stato avviato un processo di liberalizzazione del mercato mediante la progressiva abolizione dei diritti speciali ed esclusivi con lo scopo di favorire l'ingresso di nuovi operatori, e di permettere la creazione di un mercato concorrenziale, caratterizzato da una riduzione dei prezzi, un miglioramento dell'efficienza e dell'innovazione tecnologica. Per un approfondimento v. A. MANGANELLI, *Il principio di concorrenza fra antitrust e regolazione. Il caso delle comunicazioni elettroniche*, in *Conc. merc.*, 2013, da p. 279, p. 294 ss.; M. LIBERTINI, *Regolazione e concorrenza nel settore delle comunicazioni elettroniche*, in *Giornale di diritto amministrativo*, 2005, p. 195 e ss.

[2] Il modello di liberalizzazione inizialmente prescelto nel mercato delle telecomunicazioni è stato caratterizzato dal mantenimento nei mercati nazionali di un'unica infrastruttura di rete di proprietà dell'ex monopolista, seppure "aperta" ai concorrenti, ai quali veniva consentita l'utilizzazione della rete al fine di erogare i servizi ai clienti finali. Proprio per consentire l'entrata nel mercato di nuovi operatori il processo di liberalizzazione è stato, dunque, accompagnato dalla creazione di un complesso normativo regolamentare di derivazione europea volto ad imporre *ex ante* in capo all'ex monopolista legale, che continuava ad essere il detentore della rete, una serie di misure che consentissero agli *incumbent* di avere accesso alla rete. In questo senso sono state determinanti due direttive: la direttiva 90/387 CEE sull'istituzione del mercato interno per i servizi di telecomunicazione (*Open network provision*), che ha imposto l'accesso a condizioni trasparenti obiettive e non discriminatorie, e la direttiva 90/388 di liberalizzazione di tutti i servizi tranne la telefonia vocale. Il processo di liberalizzazione è stato, successivamente completato, con la direttiva 96/19/CE che ha segnato l'apertura alla concorrenza di tutti i servizi delle telecomunicazioni. L'ulteriore e decisivo passo nella creazione di un quadro normativo armonizzato ed innovativo, in quanto concernente l'interezza delle comunicazioni elettroniche, è avvenuto con il pacchetto di provvedimenti emanati nel 2002 (c.d. *New Regulatory Framework*) ed avente ad oggetto tutti i settori investiti dalle comunicazioni elettroniche, ossia le tele-

lizzarsi attraverso l'imposizione di obblighi c.d. asimmetrici, in quanto posti in capo al gestore e proprietario dell'unica infrastruttura esistente, ed aventi ad oggetto le condizioni di accesso e utilizzo della rete, con lo scopo di permettere alle altre imprese presenti nel mercato dei servizi al dettaglio di poter competere ad armi pari con l'impresa verticalmente integrata[3].

---

comunicazioni, la radiotelevisione e l'informatica. Le direttive in questione sono state: la direttiva 2002/21/CE del 7 marzo 2002 ("*direttiva quadro*"), che ha istituito un quadro normativo comune per le reti ed i servizi di comunicazione elettronica; la direttiva 2002/19/CE del 7 marzo 2002 ("*direttiva accesso*"), relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, nonché all'interconnessione delle stesse; la direttiva 2002/20/CE del 7 marzo 2002 ("*direttiva autorizzazioni*"), concernente le autorizzazioni per le reti ed i servizi di comunicazione elettronica; la direttiva 2002/22/CE del 7 marzo 2002 ("*direttiva servizio universale*"), relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica. L'impostazione di fondo accolta da tali misure normative consiste nella previsione di un *iter* volto ad accertare il livello di concorrenza dei mercati delle comunicazioni elettroniche e a valutare l'opportunità di imporre misure regolatorie *ex ante*. In particolare, l'Autorità di regolazione nazionale individua i mercati rilevanti, sulla base delle *Raccomandazioni* della Commissione, accerta se vi è un'impresa con significativo potere di mercato, e valuta se imporre gli obblighi c.d. asimmetrici volti a promuovere la concorrenza. Il recepimento dei provvedimenti europei è avvenuto in Italia con il d.lgs. del 1° agosto 2003, n. 259 recante "Codice delle comunicazioni elettroniche", così come modificato dal decreto legislativo 28 maggio 2012, n. 70, ed oggi sostituito dal d.lgs. 8 novembre 2021, n. 207. Per un approfondimento del pacchetto *NRF* v. I. Dobbs e P. Richards, *Innovation and the New Regulatory Framework for Electronic Communications in the E.U.*, in *European Competition Law Review*, 2004, p. 716 ss.; v. i saggi in G. Morbidelli e F. Donati (a cura di), *L'evoluzione del sistema delle comunicazioni elettroniche tra diritto interno e diritto comunitario*, Giappichelli, Torino, 2005; G. De Minico, *Le direttive CE sulle comunicazioni elettroniche dal 2002 alla revisione del 2006. Un punto fermo?*, in P. Costanzo, G. De Minico, R. Zaccaria, *I tre codici della Società dell'informazione*, Giappichelli, Torino, 2006, p. 169 ss.; F. Donati, *L'ordinamento amministrativo delle comunicazioni*, Giappichelli, Torino, 2007; M. Orofino, *Profili costituzionali delle comunicazioni elettroniche nell'ordinamento multilivello*, Giuffrè, Milano, 2008. Tali direttive saranno poi modificate dalle direttive nn. 2009/136/CE e 2009/140/CE adottate dal Parlamento europeo e dal Consiglio il 25 novembre 2009, il c.d. *Telecoms Package*, per un approfondimento v. M. Orofino, Il *Telecoms package: luci ed ombre di una riforma molto travagliata*, in *Riv. it. dir. pubbl. com.*, 2010, da p. 513.

[3] Gli obblighi asimmetrici previsti nei mercati dell'accesso all'ingrosso sono costituiti da: (*a*) gli obblighi di accesso alla rete ed alle risorse di rete; (*b*) l'obbligo di trasparenza; (*c*) l'obbligo di non discriminazione; (*d*) l'obbligo di controllo dei prezzi e di contabilità dei costi; (*e*) l'obbligo di separazione contabile; (*f*) l'obbligo di separazione funzionale. Si precisa che l'obbligo di separazione funzionale può essere imposto

La direttiva europea, come si approfondirà, nel prossimo paragrafo è andata, infatti, nel senso di incoraggiare una concorrenza infrastrutturale (c.d. *facilty based competition*)[4] attraverso l'alleggerimento degli obblighi regolamentari in capo alle imprese operanti esclusivamente nel mercato dell'accesso (c.d. operatore *wholesale only*), soprattutto con lo scopo di favorire lo sviluppo di *reti ad altissima capacità* (c.d. *Next generation access network*)[5].

Il recepimento nel nostro ordinamento del Codice europeo delle comunicazioni elettroniche, attraverso l'emanazione del d.lgs. 8 novembre 2021, n. 207, che ha così sostituito il d.lgs. 259/2003, ha previsto sia l'eventualità di un operatore già in origine operante nel solo mercato dell'accesso all'infrastruttura (v. art. 91), sia la possibilità di un'acquisizione successiva della qualificazione di operatore *wholesale only*, attraverso la cessione a terzi delle reti detenute, ipotesi questa specificamente regolata dall'art. 89 del Codice, che prevede una procedura per la separazione volontaria della rete da parte dell'impresa verticalmente integrata che coinvolge l'autorità di regolazione.

È allora nell'ambito di tale procedura che deve inquadrarsi propriamente l'operazione che ha portato all'acquisizione della rete fissa primaria e secondaria detenuta da Tim s.p.a.[6] da parte dei

---

quando gli altri obblighi si siano rivelati inefficienti al fine di garantire un'effettiva concorrenza sul mercato. Sul punto v. M. Orofino, *Il telecoms package*, cit., p. 529 s.; F. Dalle Nogare, *Regolazione e mercato delle comunicazioni elettroniche. La storia, la governance delle regole e il nuovo Codice europeo*, Giappichelli, Torino, 2019, p. 103 ss.

[4] Sulla concorrenza infrastrutturale v. F. Florez Duncan, R. Alimonti e S. Sharma, *Sviluppo della concorrenza infrastrutturale e regolamentazione degli oligopoli nelle comunicazioni elettroniche*, in *Merc. conc. reg.*, 2018, da p. 343.

[5] Storicamente la rete di accesso, ossia quella che provvede alla connessione della clientela alla rete, si è sviluppata impiegando prevalentemente cavi in rame a coppie simmetriche, ma, come noto, essa si sta evolvendo verso l'utilizzo di fibre ottiche; per un approfondimento degli interventi statali volti a favorire lo sviluppo delle reti ad altissima capacità, v. F. Dalle Nogare, *Regolazione e mercato*, cit., p. 149 ss.

[6] Per chiarezza, occorre precisare che la rete primaria è quella in rame e in fibra ottica che collega le centrali telefoniche ai cabinet, ovvero gli armadietti ai bordi delle strade nelle città. Essa, prima della cessione della rete, apparteneva interamente e direttamente a Tim. La rete secondaria è quella che collega l'armadietto di strada alla casa del cliente. Prima dello scorporo delle reti, la rete secondaria apparteneva indirettamente a Tim, essendo detenuta da FiberCop, che prima dell'operazione era sottoposta al controllo congiunto di Tim, con una partecipazione pari al 58% del capitale,

fondi statunitensi gestiti da Kohlberg Kravis Roberts & Co. L.P. ("KKR")[7].

In particolare, l'operazione si è perfezionata il 1° luglio 2024 attraverso l'acquisizione da parte di Optics BidCo s.p.a., appartenente al gruppo KKR, della partecipazione di maggioranza di

---

e di Teemo Bidco (società di scopo controllata dal fondo KKR) col 37,5%, mentre Fastweb S.p.A. deteneva il 4,5%. È utile ricordare che la società FiberCop s.p.a. era stata costituita nel novembre 2020, quale veicolo per la realizzazione di reti secondarie in fibra ottica, anche attraverso il lancio di un'offerta di servizi di accesso di "coinvestimento". Fino al 30 giugno 2024, FiberCop ha operato quale fornitore di servizi di accesso all'ingrosso in esclusivo riferimento alla rete secondaria.

[7] Per questa finalità, nel piano industriale di Tim 2022-2024 era stata prevista la costituzione due società: la Netco relativa alla gestione dell'infrastruttura di rete, e la Serviceco relativa alla fornitura dei servizi di telecomunicazione. L'obiettivo di tale separazione sembrava essere triplice. In primo luogo, essa mirava a superare l'integrazione verticale di Tim, qualificata come operatore con significativo potere di mercato, e per questo oggetto di obblighi regolamentari nel mercato dell'accesso. In secondo luogo, dal punto di vista finanziario l'operazione avrebbe permesso di eliminare sostanzialmente l'importante esposizione debitoria di Tim; ed in terzo luogo, l'operazione sarebbe stata funzionale alla creazione di un'infrastruttura di rete unica. In effetti, l'opzione primaria per lo scorporo di Netco era costituita da un'acquisizione da parte Open Fiber (la cui rete è in fibra ottica e non in rame), con successiva fusione con FiberCop. In questo modo si sarebbe garantita la costituzione di una rete unica, con il controllo della rete da parte dello Stato, dal momento che Open Fiber è partecipata per il 60% da Cassa Depositi e Prestiti (in mano al Ministero dell'Economia e delle Finanze con una quota dell'82,77%) e per il 40% dalla società d'investimento australiana Macquarie. Una diversa possibilità, che inizialmente sembrava meno probabile, era costituita dall'acquisizione della Netco da parte del fondo statunitense Kohlberg Kravis Roberts & Co. L.P. ("KKR"). Nei primi mesi del 2023 sono state presentate offerte non vincolanti per l'acquisizione di Netco da due soggetti: il primo costituito dal consorzio formato da CDP Equity e Macquarie Infrastructure and Real Assets (Europe) Limited; il secondo rappresentato dalla KKR. Con il comunicato del 22 giugno 2023, il consiglio di amministrazione di TIM, esaminate le offerte non vincolanti ricevute all'esito del processo competitivo, ha ritenuto preferibile l'offerta di KKR in termini di eseguibilità e relativa tempistica. Con il *Memorandum of Understanding* del 10 agosto 2023 tra il Ministero Economia e Finanze e KKR è stato siglato un accordo che prevedeva un'offerta vincolante da parte di KKR per l'acquisizione di una partecipazione di maggioranza di Netco e che contemplava, altresì, l'acquisizione da parte del MEF di una partecipazione azionaria fino al 20%. Con d.l. n. 118 del 31 agosto 2023 è stata, in effetti, autorizzata la spesa dello Stato di 2,5 miliardi di euro per l'acquisto di partecipazioni azionarie in società a rilievo strategico (corrispondente all'esborso dello Stato per acquisire una partecipazione azionaria fino al 20% del capitale di Netco). Sul cambiamento degli esiti cui avrebbe dovuto condurre la separazione della rete di Tim v. G. De Minico, *Quando prevale la logica di separare Internet e telecomunicazioni*, in *Ilsole24ore*, 30 agosto 2022.

Fibercop s.p.a., società in cui è stato contestualmente conferito il ramo d'azienda di Tim che comprendeva l'infrastruttura di rete fissa primaria e secondaria, e le attività *wholesale*. Alla data del closing, è stato altresì sottoscritto un *Master Service Agreement* ("MSA"), avente ad oggetto i termini e le condizioni dei servizi che saranno resi tra FiberCop e Tim, e che risulta funzionale a consentire a Tim, a seguito dello scorporo della rete, di procurarsi i servizi di accesso alla rete a monte, precedentemente forniti in autoproduzione dalla divisione interna *wholesale* di Tim e dalla stessa FiberCop, di cui Tim aveva il controllo.

Il *closing* è stato concluso dopo che in data 16 gennaio 2024, la Presidenza del Consiglio dei Ministri aveva approvato l'operazione con prescrizioni in forza del *golden power*, così come previsto dal decreto-legge 15 marzo 2012, n. 21, convertito, con modificazioni, dalla legge 11 maggio 2012, n. 56; e successivamente al provvedimento con cui il 30 maggio 2024 la Commissione Europea[8], nell'ambito del regolamento 139/2004 sul controllo delle operazioni di concentrazione, aveva autorizzato l'operazione senza condizioni, non avendo ritenuto che l'operazione determinasse un significativo ostacolo alla concorrenza.

Nella valutazione dell'operazione di concentrazione, la Commissione ha affermato che l'accordo *MSA* non costituiva parte integrante e necessaria dell'operazione di concentrazione e quindi non è stato autorizzato quale *ancillary restraints*, il che ha aperto la strada per una valutazione dell'accordo ai sensi del divieto delle intese restrittive della concorrenza, come di fatto poi è avvenuto con l'apertura dell'istruttoria da parte dell'Agcm[9], come approfondiremo più avanti.

L'operazione ha portato ad un nuovo assetto societario di Fibercop, che oggi si caratterizza per la perdita da parte di Tim della

[8] Commissione UE, provvedimento del 30 maggio 2024, *case* M.11386-KKR/NETCO, in cui la Commissione ha autorizzato senza condizioni l'operazione, ed ha ritenuto che gli effetti orizzontali e non orizzontali nei mercati dell'accesso determinati dall'acquisizione del controllo esclusivo di KKR su FiberCop non avrebbero determinato un ostacolo significativo alla concorrenza effettiva.

[9] AGCM, provvedimento n. 31415 del 17 dicembre 2024, di avvio dell'istruttoria ai sensi dell'art. 101 T.F.U.E., caso *I874- Master Service Agreement Tim-Fibercop*.

partecipazione societaria nel capitale di quest'ultima, e per l'assunzione da parte del gruppo KKR del suo controllo esclusivo[10].

Il venir meno – almeno in senso strutturale – dell'integrazione verticale ha fatto sorgere uno scenario del tutto nuovo nel mercato italiano delle comunicazioni in postazione fissa, imponendo una riflessione sulle conseguenze del nuovo assetto tanto per ciò che concerne gli aspetti regolamentari, quanto per ciò che riguarda le questioni concorrenziali poste dall'accordo commerciale tra Fibercop e Tim.

## 2. *Questioni regolatorie: l'operatore* wholesale only *nel Codice europeo delle comunicazioni elettroniche.*

L'obiettivo della normativa di matrice europea nel settore delle comunicazioni elettroniche è sempre stato quello di una progressiva riduzione della regolazione settoriale *ex ante* a mano a mano che si fosse sviluppata la concorrenza nel mercato dei servizi.

Ed in effetti, se si analizzano le *Raccomandazioni sui mercati rilevanti* emanate dalla Commissione, al fine di individuare i mercati le cui caratteristiche sono tali da giustificare l'imposizione di obblighi di regolamentazione *ex ante* in capo all'impresa con significativo potere di mercato[11], si può constatare come il numero degli

[10] Dal 1° luglio 2024, il Gruppo KKR ha acquisito il controllo esclusivo indiretto di FiberCop con circa il 37,8%; il restante azionariato è così diviso: il Ministero dell'Economia e delle Finanze ("MEF") detiene una partecipazione di circa il 16%; i fondi Azure Vista C 2020 S.à r.l. ("Azure Vista") e 13545369 Canada Inc. ("CPPIB") detengono ciascuno una partecipazione di circa il 17,5%; e il fondo italiano F2i Fibra S.r.l. ("F2i") è presente con una partecipazione di circa l'11,2%.

[11] La nozione di impresa con significativo potere di mercato è stata introdotta nell'art. 14, comma 2, della direttiva quadro 2002/21/CE, che – utilizzando concetti propri del diritto antitrust, elaborati nell'ambito dell'applicazione del divieto di abuso di posizione dominante – ha definito tale situazione come quella in cui un'impresa "(…) individualmente o congiuntamente con altri, gode di una posizione equivalente ad una posizione dominante ossia una posizione di forza economica tale da consentirle di comportarsi in misura notevole in modo indipendente dai concorrenti, dai clienti e, in definitiva, dai consumatori". Tale definizione è stata riprodotta nell'art. 17 del Codice delle comunicazioni elettroniche di cui al d.lgs. 259/03, ed attualmente nell'art. 74 del d.lgs. 207/21. Sull'interpretazione e l'applicazione della nozione di impresa con significativo potere di mercato v. la comunicazione della Commissione UE, 2018/C

stessi si sia drasticamente ridotto passando da diciotto nel 2003 a due nel 2020[12]: nell'ultima *Raccomandazione* del 18 dicembre 2020 n. 2245, infatti, gli unici due mercati nei quali la Commissione ha considerato opportuno un intervento regolatorio sono il mercato dei servizi di accesso locale all'ingrosso in postazione fissa (che include tutti i servizi di accesso, fisici o virtuali alle centrali locali) ed il mercato dei servizi di capacità dedicata all'ingrosso (che riguarda i segmenti terminali di linee affittate e i servizi *wholesale* di accesso a banda larga di alta qualità).

La crescita del grado di dinamismo concorrenziale nei mercati delle comunicazioni è stata ottenuta, peraltro, non solo con l'aumento delle imprese presenti nei mercati della prestazione dei servizi, ma altresì mediante l'incentivo ad uno sviluppo di una concorrenza tra imprese detentrici di infrastrutture alternative.

Già verso la fine degli anni Novanta, era apparso chiaro, infatti, che il modello di liberalizzazione consistente nell'imposizione di obblighi di accesso all'infrastruttura unica detenuta dall'ex monopolista potesse rallentare gli investimenti da parte degli altri operatori nella realizzazione di infrastrutture indipendenti ed alterna-

---

159/01, *Orientamenti per l'analisi del mercato e la valutazione del significativo potere di mercato ai sensi del quadro normativo dell'UE per le reti e i servizi di comunicazione elettronica*, in G.U.U.E., del 7 maggio 2018, C/159/01.

[12] Si consideri che nella prima Raccomandazione del 2003, la Commissione individuava diciotto mercati come suscettibili di regolamentazione *ex ante*, sette per i servizi al dettaglio e undici per i servizi all'ingrosso; la successiva del 2007, in ragione dell'evoluzione dei mercati verso condizioni di piena concorrenzialità, in particolare di quelli al dettaglio, riduceva il numero dei mercati rilevanti da diciotto a sette, di cui solo uno relativo ai servizi al dettaglio. La Raccomandazione (n. 2014/710/UE), pubblicata il 9 ottobre 2014, la terza in materia, ha ridotto ulteriormente il numero dei mercati soggetti a regolamentazione, escludendo dalla lista l'unico mercato al dettaglio che era rimasto nella precedente Raccomandazione e ridefinendo, al contempo, alcuni mercati all'ingrosso per tenere conto dell'andamento del settore e dell'evoluzione tecnologica. In particolare, la Raccomandazione 2014/710/UE ha individuato quattro mercati all'ingrosso suscettibili di regolamentazione *ex ante*, mantenendo nella lista i mercati dei servizi di terminazione delle chiamate su rete fissa e su rete mobile (servizi di interconnessione) e rimodulando i mercati dei servizi di accesso alla rete fissa attraverso l'individuazione di tre mercati rilevanti (il mercato 3a dei servizi di accesso locale all'ingrosso in postazione fissa, il mercato 3b dei servizi di accesso centrale all'ingrosso in postazione fissa per i prodotti di largo consumo e il mercato 4 dei servizi di accesso all'ingrosso di alta qualità in postazione fissa, corrispondenti ai segmenti terminali di linee affittate).

tive, generando un circolo vizioso a detrimento dello sviluppo tecnologico della rete esistente. È stato, infatti, posto in luce come le condizioni economiche vantaggiose per l'accesso alla rete abbiano l'effetto di disincentivare gli investimenti per la realizzazione di nuove infrastrutture da parte degli operatori alternativi, e conseguentemente determinino una scarsa propensione per il titolare della rete ai miglioramenti nella qualità e nell'innovazione della rete, giacché, da un lato, deve sopportare gli oneri economici di un miglioramento della rete di cui si avvantaggiano anche gli altri, e dall'altro, non subisce la pressione competitiva di altri operatori detentori della rete[13].

Per contenere tali conseguenze, già a partire dal pacchetto di misure del 2002 fu adottata una soluzione per conciliare due diversi modelli di sviluppo della concorrenza nel settore delle comunicazioni elettroniche, ossia il modello *service and access based competition* e il modello *faclilty based competition.* In particolare, si è voluta introdurre una regolamentazione del settore che fosse coerente con la teoria della scala di investimenti (c.d. *ladder of investments*), che si basa su una differenziazione dei servizi di accesso *wholesale* in ragione del livello di investimento progressivo nell'infrastruttura realizzato dagli operatori concorrenti all'*incumbent*, e al grado di indipendenza che tale investimento consente di raggiungere[14]. L'idea

[13] Sugli effetti negativi che la regolamentazione può avere nello sviluppo di reti alternative da parte dei concorrenti dell'impresa *incumbent*, detentrice della rete, v. C. CAMBINI e Y. JIANG, *Broadband investment and regulation: A literature review*, in *Telecommunications Policy*, vol. 33, fasc. 10-11, 2009, p. 559 ss.

[14] Il modello della scala degli investimenti è stato teorizzato da un gruppo di studiosi, tra cui in particolare Martin Cave, ed ebbe una grandissima influenza sulla Commissione europea, e in generale sui regolatori dei diversi Stati membri. La prima teorizzazione può essere rinvenuta nel contributo M. CAVE e L. PROSPERETTI, *European Telecommunications Infrastructures*, in *Oxford Review of Economic Policy*, vol. 17, 2001, p. 416 ss. Per un affinamento della teorizzazione del modello v. altresì M. CAVE e I. VOGELSANG, *How access pricing and entry interact*, in *Telecommunications Policy*, Vol. 27, Issues 10-11, 2003, p. 717 ss.; nonché lo scritto più completo M. CAVE, *Encouraging infrastructure competition via the ladder of investment*, in *Telecommunications Policy*, Vol. 30, 2006, p. 223 ss. L'idea è che i potenziali nuovi entranti nel mercato possano investire in maniera incrementale nella loro rete, piuttosto che costruirla dal nulla. L'accoglimento del principio della scala degli investimenti nelle politiche regolatorie europee appare del tutto evidente se si legge il documento presentato dall'European Regulators Group, *Erg Common Position on the approach to appropriate remedies*

della scala degli investimenti costituisce, dunque, una metafora del processo di graduale infrastrutturazione degli operatori alternativi, rappresentato come un'ascesa su una scala in cui ogni "gradino" costituisce una diversa opzione di accesso alla rete dell'ex monopolista (resa disponibile dalla regolazione), corrispondente a un livello crescente di investimenti: dalla semplice rivendita di servizi che necessita di un' infrastruttura minima, passando per una parziale infrastrutturazione, attraverso l'accesso disaggregato alla rete locale dell'ex monopolista, ed arrivando alla cima della scala mediante lo sviluppo di una rete proprietaria alternativa.

Il quadro regolatorio della prima decade degli anni Duemila è costruito intorno a questo modello, e si caratterizza per la previsione da parte delle Autorità Nazionali di Regolazione di prezzi di accesso progressivamente più bassi quanto maggiore è il livello di infrastrutturazione alternativa realizzata dai concorrenti. Lo strumento principale di questa strategia è stato l'*unbundling* della rete, vale a dire la sua apertura a vari livelli e la regolazione delle tariffe e dei modi di interconnessione[15].

---

*in the new regulatory framework*, Erg (03) 30 rev. 1, 2004, p. 13, in cui si afferma "In order to promote sustainable, infrastructure-based competition, NRAs have to set investment incentives such that the dominant undertaking's infrastructure is replicated wherever this is technically feasible and economically efficient within a reasonable period of time. Investment incentives are particularly relevant in the context of access regulation. By the decision as to if and on which level of the infrastructure access has to be provided by the SMP undertaking and by setting the access price, NRAs will influence investment incentives of both the SMP undertaking and alternative operators. Given that the cost structure and investment incentives of alternative operators are likely to change over time as they develop their trademark and a customer base, NRAs may consider to give them the possibility to take their investments in a step-by-step manner. This approach, where two or more access products at different levels of the network hierarchy are simultaneously available to alternative operators has been called the 'ladder of investment'.

[15] Cfr. M. OROFINO, *Il* Telecoms Package, cit., p. 530 s. Per un chiarimento sugli strumenti regolatori che si rifanno al principio della scala degli investimenti v. F. DALLE NOGARE, *Regolazione e mercato*, cit., p. 89 s., in cui spiega come rispetto all'accesso disaggregato c.d. *ULL*, *unbundling local loop*, l'Agcom ha proceduto a fissare un prezzo di accesso alla rete di Telecom orientato al costo, stante gli elevati costi di realizzazione dell'infrastruttura per l'accesso completamente disaggregato, mentre ha previsto prezzi più onerosi per gli accessi sostitutivi e meno infrastrutturati quali il servizio di *Wholesale line rental*, che consiste nel servizio di vendita all'ingrosso del canone di accesso,

Lo scopo di tale modello era, nel breve periodo, quello di creare una concorrenza immediata nel mercato dei servizi agli utenti finali, favorendo l'accesso nel mercato mediante l'utilizzazione della rete dell'ex monopolista legale, sì da permettere un consolidamento della posizione mediante l'acquisizione di una base di clienti. Nel lungo periodo, l'obiettivo era di promuovere la risalita della scala degli investimenti, sì da rendere vantaggioso il graduale processo di affrancazione dei nuovi entranti rispetto all'utilizzazione della rete dell'ex monopolista legale, e permettere in tal modo una concorrenza effettiva tra infrastrutture di rete alternative[16].

Il raggiungimento di tali obiettivi è stato, peraltro, non omogeneo tra i diversi Stati membri, giacché solo in alcuni Stati sono state realizzate reti alternative, e soltanto parziale, nel senso che, mentre nei gradini più bassi della scala degli investimenti il modello ha stimolato l'investimento nelle infrastrutture necessarie, tuttavia, esso non ha portato ad una completa risalita della scala, con la realizzazione di una rete del tutto indipendente[17]. Tale esito non ha permesso, dunque, di evitare gli effetti negativi del modello basato sugli obblighi di accesso alla rete, consistenti nello scarso incentivo da parte del detentore della rete ad investire nell'innovazione tecnologica e nella qualità della rete[18].

Il panorama è complessivamente mutato grazie all'avvento delle nuove tecnologie e alla realizzazione di reti di nuova generazione a banda ultra-larga, che utilizzano, in tutto o in parte, materiale in fibra ottica[19].

---

e consente agli operatori interconnessi di fornire ai propri clienti sia l'accesso alla rete telefonica sia il servizio di traffico telefonico, e di inviare agli stessi una sola fattura.

[16] Sul punto v. F.F. Duncan, R. Alimonti, e S. Sharma, *Sviluppo della concorrenza infrastrutturale*, cit., p. 343.

[17] Si veda per questa analisi i risultati del *Documento di analisi n. 32*, dell'Ufficio Valutazione Impatto del Senato della Repubblica, a cura di A. Manganelli, *La regolazione delle reti fisse di comunicazione elettronica. Effetti sullo sviluppo delle infrastrutture e dei servizi*, 2025, disponibile all'indirizzo *https://www.senato.it/application/xmanager/projects/leg19/attachments/documento/files/000/112/815/DA32_Dossier_Reti_fisse_di_comunicazione_elettronica.pdf*, p. 25 ss.

[18] Per una critica alla teoria della scala degli investimenti v. M. Bourreau, P. Doğan, M. Manant, *A critical review of the "ladder of investment" approach*, in *Telecommunications Policy*, vol. 34, 2010, p. 683 ss.

[19] Sulla considerazione secondo cui la concorrenza infrastrutturale è stata incentivata non già dalla regolazione sull'accesso, bensì da altri fattori quali la competizione

Di qui, l'approccio seguito nel nuovo Codice Europeo delle Comunicazioni elettroniche è stato quello di prevedere strumenti diversificati per incentivare gli investimenti nella realizzazione di reti di nuova generazione. Tra queste misure rientrano, senza dubbio, gli accordi di coinvestimento tra operatori nelle reti ad altissima capacità (di cui all'art. 76 dir. UE 2018/1972, e recepito nell'art. 87 del d.lgs. 207/2021), la cui finalità è quella di offrire vantaggi significativi in termini di condivisione di costi e rischi, consentendo così anche alle imprese di dimensioni minori di investire a condizioni economicamente convenienti e di acquisire diritti specifici di carattere strutturale sulla rete, incentivando una concorrenza sostenibile a lungo termine anche in aree in cui non risulti ancora effettiva una concorrenza basata su un'offerta diversificata di reti di nuova generazione. Rispetto a tali accordi, la normativa si preoccupa di proteggere gli interessi degli operatori richiedenti l'accesso alla rete che non partecipano al coinvestimento, i quali vengono tutelati attraverso l'obbligo di mantenere le condizioni di accesso già esistenti o, nel caso in cui ciò non sia possibile in quanto elementi di rete preesistenti sono destinati ad essere smantellati, mediante l'imposizione di prodotti di accesso aventi funzionalità e qualità analoghe a quelli precedentemente disponibili[20].

Tra gli strumenti volti ad incoraggiare l'investimento nella realizzazione delle reti di nuova generazione deve farsi rientrare anche l'alleggerimento degli obblighi di regolazione in capo all'impresa titolare della rete, che abbia un significativo potere di mercato nel mercato *wholesale* dell'accesso, ma che non sia presente nei mercati dei servizi al dettaglio (c.d. operatore *wholesale only*).

In particolare, ai sensi dell'art. 80 della Dir. Ue 2018/1972, riprodotto nell'art. 91 del d.lgs. 207/2021, ai fini della qualificazione di un'impresa come attiva esclusivamente sul mercato all'ingrosso devono ricorrere due condizioni: (*a*) l'impresa medesima, le società appartenenti al gruppo, le sue unità commerciali, le società di cui

---

delle reti via cavo e delle reti alternative in fibra ottica, e altresì dall'effetto sostitutivo incrementale delle reti fisse con le reti mobili, F.F. Duncan, R. Alimonti, e S. Sharma, *op. cit.*, p. 348 ss.

[20] Sul punto v. F. Dalle Nogare, *Vigilanza e impegni sulla rete unica. Una partita a due*, in *Merc. conc. reg.*, 2021, p. 159.

abbia anche il controllo congiunto, nonché qualsiasi azionista in grado di esercitare un controllo sull'impresa, devono svolgere attività, attuali e previste per il futuro, *solo nei mercati all'ingrosso* dei servizi di comunicazione elettronica e pertanto non devono svolgere alcuna attività in un mercato al dettaglio dei servizi di comunicazione elettronica forniti agli utenti finali; (*b*) l'impresa non deve avere l'obbligo di contrattare, in forza di un contratto di esclusiva o di un accordo che di fatto costituisca un'esclusiva, con un'unica impresa separata operante a valle che sia attiva in un mercato al dettaglio dei servizi di comunicazione elettronica forniti a utenti finali.

Laddove ricorrano entrambe le condizioni, e l'impresa abbia un significativo potere di mercato, l'Autorità di regolazione nazionale potrà imporre – ma solo se lo ritenga opportuno in base ad un valutazione anche prospettica del comportamento dell'impresa – soltanto alcuni degli obblighi di carattere asimmetrico, ossia in particolare potrà imporre l'obbligo di non discriminazione e di accesso (ai sensi rispettivamente degli artt. 81, e 84 d.lgs. 207/2021), o anche l'obbligo di prevedere prezzi equi e ragionevoli, ma non potrà imporre gli obblighi di trasparenza (art. 80), di separazione contabile (art. 82), di accesso alle infrastrutture di ingegneria civile (art. 83), e di controllo dei prezzi e contabilità dei costi (art. 85).

Occorre, peraltro, considerare che, laddove in ragione delle condizioni praticate, possano verificarsi problemi concorrenziali che pregiudichino i clienti finali, l'Agcom potrà ampliare gli obblighi gravanti sull'operatore *wholesale only*, imponendo anche uno o più degli obblighi asimmetrici di cui agli artt. 80-85 del d.lgs. 207/2021, e quindi anche quelli normalmente esclusi per l'impresa non verticalmente integrata.

### 3. (*Segue*) *La qualificazione di FiberCop come operatore* wholesale only *e gli obblighi regolamentari nei mercati dell'accesso all'ingrosso*

La perdita, a seguito della cessione della rete, della strutturale integrazione verticale di Tim, che, in quanto impresa con significativo potere di mercato, era soggetta agli obblighi di carattere asimmetrico per consentire l'accesso alla rete a parità di condizioni agli

operatori alternativi, ha reso del tutto incerto il quadro regolatorio, rendendo necessaria una nuova definizione dello stesso. Il mutato assetto del mercato all'ingrosso ha imposto, infatti, in primo luogo, di valutare se Fibercop possa essere considerata un'impresa operante soltanto nel mercato dell'accesso all'ingrosso; in secondo luogo, di accertare la situazione concorrenziale dei mercati, al fine di verificare se Fibercop possa essere considerata come impresa con significativo potere di mercato, e quindi destinataria di misure regolamentarie; ed in terzo luogo, in caso di risoluzione positiva delle prime due questioni, di valutare quali obblighi imporre alla medesima ai sensi dell'art. 91 del Cod. Com. El.

D'altro canto, si è resa necessaria anche la valutazione della nuova posizione di Tim, sì da verificare la sorte degli obblighi regolamentari antecedentemente previsti in capo alla medesima nei servizi *retail*.

Prendendo le mosse dai mercati dell'accesso all'ingrosso, appare opportuno brevemente ricordare gli esiti delle più recenti analisi di mercato compiute dall'Agcom, prima dell'operazione di dismissione volontaria della rete da parte di Tim.

In particolare, nelle delibere 348/19/CONS[21] e 333/20/CONS[22], l'Agcom aveva previsto la necessità di una regolazione *ex ante* in tre mercati *wholesale*, ossia quello dell'accesso locale e del-

[21] Delibera Agcom, del 17 luglio 2019, n. 348/19/CONS, in cui l'Autorità ha qualificato Tim come operatore con significativo potere di mercato nel mercato dell'accesso centrale all'ingrosso e nel mercato dell'accesso locale all'ingrosso alla rete telefonica pubblica in postazione fissa sia su rete in rame sia su rete in fibra ottica forniti nei Comuni italiani, con l'eccezione del Comune di Milano, considerato come mercato distinto geograficamente per le sue condizioni di sviluppo della concorrenza, nell'ambito del quale si è ritenuto non vi fossero condizioni per imporre obblighi regolamentari *ex ante*.

[22] Delibera Agcom del 22 luglio 2020, n. 333/20/CONS, in cui l'Agcom ha qualificato Tim come operatore con significativo potere di mercato nell'accesso all'ingrosso di alta qualità in postazione fissa destinata alla clientela affari, comprensivo dei circuiti di capacità dedicata (da intendersi non condivisa con altri servizi all'interno dello stesso flusso numerico, se del caso, a pacchetti) tra un punto di attestazione di un operatore alternativo presso un nodo della rete dell'operatore che offre il servizio e una sede d'utente. L'Agcom ha ritenuto, peraltro, che anche rispetto a questo mercato il Comune di Milano costituisse un mercato separato, nell'ambito del quale ha considerato che Tim non potesse qualificarsi come un operatore con significativo potere di mercato.

l'accesso centrale all'ingrosso, nonché nel mercato della fornitura del servizio di accesso di alta qualità in postazione fissa, con l'esclusione del Comune di Milano considerato come un mercato rilevante distinto dal resto d'Italia.

Con la successiva delibera 114/24 CONS[23], l'Agcom ha rimosso il mercato dell'accesso centrale all'ingrosso dai mercati oggetto di regolazione *ex ante*, in conformità di quella che era stata l'indicazione della *raccomandazione* n. 2020/ 2245 della Commissione europea, del 18 dicembre 2020, e pertanto ha revocato gli obblighi regolamentari precedentemente imposti a Tim in questo mercato.

Nel medesimo provvedimento ha, invece, confermato la posizione di significativo potere di mercato di Tim, unitamente alla controllata Fibercop attiva nel mercato dell'accesso alla rete secondaria, in due mercati, ossia quello dell'accesso locale all'ingrosso e quello della fornitura del servizio di accesso di alta qualità in postazione fissa, con l'eccezione di alcune aree geografiche ritenute pienamente concorrenziali. Conseguentemente, per le restanti aree geografiche del Paese sono stati confermati gli obblighi regolamentari, ossia in particolare gli obblighi di: (*i*) accesso alle infrastrutture di ingegneria civile; (*ii*) accesso ed uso di determinate risorse di rete[24]; (*iii*) traspa-

[23] Delibera del 30 luglio 2024, n. 114/24/CONS, che si caratterizza per una diversa identificazione dei mercati geografici ritenuti pienamente concorrenziali (individuati in quattordici Comuni per il mercato dei servizi di accesso locale e quattro Comuni per quello dei servizi di capacità dedicata) nei quali sono stati revocati gli obblighi regolamentari, e per l'individuazione di aree maggiormente contendibili (novantacinque Comuni per il mercato dei servizi di accesso locale e sessantasette Comuni per quello dei servizi di capacità dedicata) in cui è stata sospesa l'applicazione dell'obbligo del controllo dei prezzi.

[24] Sotto il profilo degli obblighi concernenti l'accesso a risorse di rete, gravava su Tim, quale operatore dotato di significativo potere di mercato nei mercati dell'accesso, l'obbligo della fornitura dei seguenti servizi di accesso locale: (*i*) accesso completamente disaggregato alla rete locale in rame (ULL); (*ii*) accesso disaggregato alla sottorete locale in rame (SLU); (*iii*) accesso alle infrastrutture di posa; (*iv*) accesso alla fibra spenta nelle tratte di rete primaria e secondaria; (*v*) accesso al segmento di terminazione, (*vi*) accesso disaggregato alla rete in fibra ottica a livello di centrale locale, laddove ciò risulti essere tecnicamente possibile; (vii) l'accesso disaggregato virtuale (c.d. VULA), che consiste nella fornitura dell'accesso virtuale alla rete locale che comprende la fornitura della capacità trasmissiva dalla sede dell'abbonato alla centrale locale della rete in fibra.

renza; (*vi*) non discriminazione[25]; (*v*) separazione contabile; (*vi*) controllo dei prezzi e contabilità dei costi[26].

Sotto il profilo dell'obbligo di non discriminazione, occorre porre in rilievo fin d'ora, giacché ritorneremo sul punto nel prosieguo, che, al fine di verificare le eventuali discriminazioni commesse dall'operatore con significativo potere di mercato, l'Autorità di regolazione aveva previsto in capo a Tim l'obbligo di comunicazione preventiva delle offerte praticate nei servizi *retail*, in modo da permettere la verifica della loro replicabilità, sia tecnica che economica, da parte degli altri operatori.

Al fine di valutare gli effetti della vendita al gruppo KKR della rete primaria e secondaria, l'Agcom, in data 11 settembre 2024, ha avviato, ai sensi dell'art. 89, comma 2, del codice di comunicazioni elettroniche, un'istruttoria volta a decidere se imporre, mantenere, modificare o rimuovere gli obblighi regolamentari[27].

Essendo, peraltro, propedeutica a questo accertamento la questione della qualificazione di Fibercop come operatore *wholesale only* ai sensi dell'art. 91, Cod. Com. El., l'Agcom ha avviato con de-

---

[25] Rispetto all'obbligo di non discriminazione è stato confermato il modello di *equivalence* potenziato adottato con la delibera Agcom 652/16/Cons che prevede una serie di impegni volti a garantire la parità di trattamento tra la propria divisione commerciale e gli altri operatori che acquistano i servizi di accesso all'ingrosso per fornire i servizi al dettaglio ai clienti finali. Nel monitoraggio sul rispetto degli obblighi di non discriminazione l'Agcom si è avvalsa dell'Organo di Vigilanza, ossia un organo interno alla *governance* societaria di Tim, dotato di autonomia e indipendenza, cui è affidato il compito di vigilare sulla corretta esecuzione degli Impegni e sugli obblighi di non discriminazione, istituito il 1° aprile 2009 conformemente a quanto stabilito dagli Impegni presentati da Tim ai sensi della Legge n. 248/06 e approvati dall'Autorità per le garanzie nelle comunicazioni con delibera n. 718/08/CONS. Di propria iniziativa o su segnalazione di terzi, procede alla verifica della loro eventuale violazione, comunicandola all'Autorità per le garanzie nelle comunicazioni e al Consiglio di Amministrazione di Tim, acquisendo le informazioni e i dati necessari allo svolgimento delle proprie funzioni presso tutte le strutture di Tim coinvolte nel processo.

[26] Con specifico riferimento all'implementazione dell'obbligo di controllo dei prezzi, l'Autorità ha confermato l'obbligo dei prezzi di accesso orientati ai costi, mentre per i Comuni definiti contendibili ha previsto l'applicazione da parte di Tim di prezzi equi e ragionevoli.

[27] Il procedimento di cui all'art. 89, comma 2, cod. com. elettr., prevede in particolare che, nella valutazione degli effetti della separazione volontaria della rete ai fini della determinazione degli obblighi regolamentari, l'Agcom debba consultare le imprese terze interessate, ed inoltre acquisire preventivamente il parere dell'Agcm.

libera 103/25/CONS del 16 aprile 2025, una consultazione pubblica avente ad oggetto, in particolare, la valutazione della ricorrenza delle due condizioni necessarie per escludere l'operatività nel mercato dei servizi al dettaglio, ossia: (*a*) la non operatività dell'impresa (anche attraverso controllate e controllanti) nei mercati *retail* dei servizi di comunicazione elettronica; (*b*) la mancanza di relazioni contrattuali di fornitura "esclusiva" con imprese che operano nei mercati *retail*.

Nell'ambito della consultazione pubblica, sono state avanzate da parte degli operatori alternativi posizioni critiche rispetto alla ricorrenza della suddette condizioni, in ragione in particolare delle clausole previste nel contratto di *Master Service Agreement* concluso tra FiberCop e Tim, ritenute idonee a determinare un livello di integrazione tale da impedire che l'impresa attualmente detentrice della rete, ossia FiberCop, possa essere considerata come un'impresa che opera soltanto nei servizi all'ingrosso. Molti operatori hanno, infatti, rilevato come dalle clausole in esso previste derivi un legame equivalente all'esclusiva, e permanga una integrazione verticale di fatto, per la circostanza che i servizi venduti a Tim costituiscono la parte più significativa e irrinunciabile del volume di affari di FiberCop.

La valutazione dell'Agcom, sulla quale è stato dato parere adesivo dall'Agcm, è andata, invece, nel senso di ritenere soddisfatte entrambe le condizioni, non sussistendo legami partecipativi da parte del gruppo KKR in società operanti nel mercato dei servizi al dettaglio, e non risultando esservi, alla luce del contratto di *MSA*, rapporti di fornitura esclusiva tra Fibercop e Tim in ordine ai servizi di comunicazione elettronica nei mercati all'ingrosso.

Alla luce di tale valutazione, nello schema del nuovo provvedimento sull'analisi dei mercati, sottoposto a consultazione pubblica con delibera 205/25/CONS, l'Agcom ha previsto rispetto ai mercati dell'accesso locale all'ingrosso e dei servizi di fornitura di capacità dedicata di alta qualità in postazione fissa, eccezion fatta per alcune aree geografiche ritenute concorrenziali, di prevedere in capo a FiberCop, in quanto operatore con significativo potere di mercato: (*i*) gli obblighi di accesso all'infrastrutture di ingegneria civile e alle risorse di rete, nonché, (*ii*) l'obbligo di non discriminazione, (*iii*) l'obbligo di accessi a prezzi equi.

Con riguardo all'obbligo di non discriminazione, in particolare, l'Agcom ha rilevato che, sebbene sia venuta meno l'integrazione verticale tra l'operatore con significativo potere di mercato nell'accesso all'ingrosso e l'operatore con significativo potere di mercato nei servizi al dettaglio in postazione fissa, in ogni caso l'operatore *wholesale only* potrebbe sfruttare la propria condizione di dominanza nei mercati dei servizi di accesso locale all'ingrosso e a capacità dedicata, accordando l'accesso a condizioni discriminatorie a vantaggio di un singolo operatore e discapito di altri, ostacolando dunque la competitività di questi ultimi. Per tale ragione, ha previsto che FiberCop debba fornire agli operatori alternativi l'accesso ai servizi all'ingrosso, in maniera non discriminatoria, ossia a condizioni economiche e tecniche equivalenti in circostanze equivalenti, adottando e rendendo disponibili a tutti i richiedenti l'accesso le stesse informazioni, gli stessi sistemi, processi e banche dati[28].

Inoltre, al fine di permettere la valutazione del rispetto degli obblighi di non discriminazione, è previsto in capo a Fibercop l'obbligo di comunicare all'Agcom e pubblicare sul proprio sito le offerte praticate, dando evidenza dei listini, con validità annuale o pluriennale, concernenti le condizioni tecniche, economiche e procedurali, sufficientemente dettagliate e disaggregate, in base ai diversi servizi di accesso.

L'Agcom ha, altresì, previsto in capo a Fibercop l'obbligo di prevedere *prezzi equi e ragionevoli* per l'accesso alle risorse di rete nei mercati oggetti di intervento regolatorio. Tale imposizione è ricondotta all'esigenza di evitare comportamenti anticompetitivi da

[28] Con riferimento alle condizioni economiche di fornitura, ne discende l'obbligo in capo a FiberCop di applicare prezzi uguali a condizioni equivalenti a tutti gli operatori richiedenti l'accesso, anche nel caso di regimi di sconti o condizioni particolari, che dovranno essere valutati dall'Agcom. Con riferimento alle condizioni tecniche di fornitura dei servizi di accesso all'ingrosso, FiberCop dovrà garantire l'impiego delle medesime tecnologie a tutti gli operatori richiedenti accesso, garantendo i medesimi tempi di *provisioning* (consistente nell'attivazione di nuove linee o di linee per utenti migrati) e *assurance* (concernente i servizi di manutenzione e riparazione delle risorse di rete). Nello schema di provvedimento, l'Agcom ha previsto che l'Organismo di Vigilanza debba coadiuvare FiberCop al fine di attuare un modello di trattamento equivalente, quale quello che aveva caratterizzato Tim prima della cessione della rete.

parte dell'operatore *wholesale only*, in quanto, nonostante l'operazione di separazione, potrebbe adottare strategie escludenti, fornendo, da un lato, l'accesso alla rete a condizioni economiche non ragionevoli, laddove la pressione concorrenziale è più bassa, e imponendo, dall'altro, prezzi predatori nelle aree in cui sono presenti offerte all'ingrosso alternative.

Dallo schema di provvedimento dell'Agcom può, allora, osservarsi come, sebbene si valuti Fibercop come operatore attivo soltanto nel mercato all'ingrosso, e quindi necessariamente vi sia un alleggerimento degli obblighi regolamentari, essendo stati revocati del tutto gli obblighi di trasparenza, contabilità dei costi e separazione contabile, siano stati imposti, comunque, obblighi regolamentari superiore al livello minimo richiesto dall'art. 91 Cod. Com. El., essendo stati previsti, oltre agli obblighi di non discriminazione (art. 81) e di accesso e uso di determinati elementi di rete e risorse correlate (art. 84) anche il rispetto dell'obbligo di accesso alle infrastrutture di ingegneria civile (art. 83), e di previsione di prezzi equi e ragionevoli.

Tale valutazione complessiva può dirsi apprezzabile, in quanto tiene conto, da un lato, dell'attuale permanenza delle condizioni del *Master Service Agreement*, e dall'altro dell'estrema novità della situazione, che richiederà una valutazione nel tempo dei possibili effetti sul mercato, come previsto dall'art. 91, comma 4, che consente di graduare l'imposizione di obblighi regolamentari all'impresa *wholesale only* tenendo conto dei problemi concorrenziali che potrebbero sorgere a scapito degli interessi dei clienti finali.

## 4. (*Segue*) *La valutazione della posizione di Tim e gli obblighi di verifica di replicabilità delle offerte*

Prima della cessione della rete al gruppo KKR, Tim, quale operatore con significativo potere di mercato verticalmente integrato, era destinataria di obblighi regolamentari non solo sul mercato dell'accesso, ma anche nel mercato al dettaglio.

In particolare, al fine di rendere effettivo l'obbligo di non discriminazione, l'Autorità garante per le comunicazioni ha ritenuto

necessaria l'applicazione dei test di replicabilità su tutte le offerte dei servizi di accesso al dettaglio di Tim, in modo da consentire la verifica della riproducibilità economica e tecnica delle offerte da parte di un operatore altrettanto efficiente[29].

In ragione di ciò Tim era, dunque, tenuta a comunicare all'Autorità le nuove condizioni di offerta dei servizi di accesso al dettaglio, nonché le modifiche alle condizioni di offerta preesistenti, con almeno 20 giorni di anticipo rispetto alla data prevista per la loro commercializzazione.

In seguito alla cessione della rete, e conseguentemente in ragione del venir meno dell'integrazione verticale, Tim ha presentato istanza al fine di ottenere in via cautelare la sospensione dell'obbligo di comunicazione delle offerte di accesso al dettaglio.

Nonostante le ragioni contrarie sollevate dagli operatori alternativi, e fondate sul mantenimento di un'integrazione verticale di fatto tra Fibercop e Tim dovuta alle clausole del *Master Service Agreement*, l'Agcom, con delibera del 406/24/CONS del 23 ottobre 2024, ha accolto l'istanza di sospensione cautelare, revocando così in capo a Tim gli obblighi di replicabilità delle offerte nel mercato al dettaglio.

In particolare, l'Agcom ha precisato come l'imposizione di tale obbligo avesse trovato la propria *ratio* giustificatrice nella circostanza che l'operatore avente significativo potere di mercato nei mercati all'ingrosso fosse anche operatore integrato verticalmente nei corrispondenti mercati al dettaglio, in quanto, attraverso le verifiche di replicabilità delle offerte al dettaglio di Tim, il regolatore avrebbe potuto individuare le eventuali discriminazioni commesse dall'operatore con significativo potere di mercato nei mercati dei servizi di accesso all'ingrosso. L'Autorità ha, altresì, osservato che l'analisi delle clausole del *MSA* avrebbe assunto rilevanza ai fini della qualificazione di Fibercop come operatore *wholesale only*, e quindi al fine di individuare gli obblighi regolamentari imponibili nei mercati dell'accesso all'ingrosso, ma in nessun modo avrebbe

[29] Da ultimo, la verifica della replicabilità delle offerte di Tim nei servizi dell'accesso al dettaglio è stata confermata nella delibera 114/24/CONS, negli artt. 10, comma 9, 37 e 38.

potuto portare al mantenimento di obblighi regolamentari in capo a Tim, divenuto soggetto acquirente dei servizi di accesso all'ingrosso da Fibercop, ed operante, dal lato dell'offerta, unicamente nei mercati attualmente definiti come non suscettibili di regolamentazione *ex ante*.

Tale valutazione è stata confermata nello schema di delibera sottoposto a consultazione pubblica con provvedimento 205/25/CONS, in cui, oltre all'indicazione delle misure regolamentari imposte a Fibercop quale operatore *wholesale only* con significativo potere di mercato su cui ci siamo soffermati nel paragrafo precedente, l'Agcom ha revocato in via definitiva gli obblighi di Tim inerenti alla replicabilità delle offerte al dettaglio. In particolare, l'Autorità di regolazione ha precisato che la cessione dell'infrastruttura di accesso fissa di Tim a FiberCop, nonché la natura di operatore *wholesale only* di FiberCop, ha fatto venir meno la *ratio* dell'obbligo, ed ha comportato la perdita di significatività della metodologia dei test di prezzo sull'offerta di servizi al dettaglio da parte di Tim.

L'Agcom ha, infine, chiarito che gli obblighi regolamentari *ex ante*, imponibili ai sensi del Codice delle Comunicazioni elettroniche sono prerogativa dell'operatore individuato quale detentore di significativo potere di mercato nei due mercati rilevanti dei servizi di accesso all'ingrosso (quelli dell'accesso locale all'ingrosso e quello dei servizi a capacità dedicata in postazione fissa), ossia – attualmente – FiberCop; ed ha, altresì, posto in luce che con la perdita dell'integrazione verticale sono venuti meno i presupposti giuridici per il mantenimento, in capo a Tim, di obblighi asimmetrici connessi ad una condizione di significativo potere nei mercati dei servizi di accesso all'ingrosso alla rete fissa, che non detiene più.

In considerazione delle analisi compiute dall'Agcom nella valutazione delle esigenze di regolazione *ex ante* dei mercati, e della conseguente conformazione degli obblighi regolamentari, di cui si attende la conferma all'esito della consultazione pubblica, appare cruciale, allora, la valutazione delle criticità di carattere concorrenziale che possono discendere dalle clausole del contratto di *Master Service Agreement* concluso tra Fibercop e Tim, su cui appare allora necessario soffermarsi.

## 5. *Questioni concorrenziali: il Master Service Agreement e il divieto di intese restrittive*

Come già rilevato precedentemente, la Commissione europea, al momento della valutazione della compatibilità dell'operazione di concentrazione tra KKR e Tim e consistente nell'acquisizione del controllo esclusivo di Fibercop, cui sono stati assegnati tutti gli assets di rete primaria e secondaria in postazione fissa, ha ritenuto che le previsioni del contratto regolante la fornitura di servizi tra Fibercop e Tim (c.d. *Master Service Agreement*) non potessero essere considerate come *ancillary restraints*, ossia come restrizioni concorrenziali necessarie per la realizzazione dell'operazione, e pertanto ha lasciato aperta la possibilità della valutazione dei loro effetti anticoncorrenziali.

Tale considerazione appare del tutto coerente con l'approccio fatto proprio dalla Commissione nella Comunicazione sulle restrizioni direttamente connesse con l'operazione di concentrazione[30], in cui si chiarisce che possono essere considerate tali soltanto quelle limitazioni che, nel caso in cui non esistessero, non permetterebbero di realizzare l'operazione o permetterebbero di realizzarla soltanto in condizioni assai più aleatorie, a costi sostanzialmente più elevati, in tempi nettamente più lunghi o con ben minori possibilità di successo.

Con specifico riguardo ai casi di scorporo di un'impresa o di parti di essa, la Commissione ha anche ritenuto ammissibili come restrizioni necessarie gli accordi di fornitura ed acquisto caratterizzati da esclusiva tra acquirente e venditore, in ragione del fatto che essi permettono di garantire la continuità di approvvigionamento per i prodotti necessari allo svolgimento delle attività mantenute dal venditore o rilevate dall'acquirente. La Commissione ha, tuttavia, precisato che potrebbero essere ritenute strettamente necessarie soltanto le clausole volte a fissare dei quantitativi di fornitura *indispensabili al mantenimento della continuità aziendale* e per un periodo limitato e non superiore a cinque anni. L'autorità europea ha,

[30] Commissione EU, *Comunicazione della Commissione sulle restrizioni direttamente connesse e necessarie alle concentrazioni*, 2005/C 56/03, in G.U.U.E del 5 marzo 2005.

altresì, chiarito come gli obblighi che comportano quantitativi illimitati o l'esclusiva o che conferiscono uno *status* di fornitore o acquirente privilegiato non possono considerarsi necessari alla realizzazione della concentrazione[31].

La mancata qualificazione del contenuto del *MSA* come restrizione direttamente connessa e necessaria ha portato l'Agcm ad avviare, con provvedimento del 17 dicembre 2024[32], un'istruttoria volta a verificare se le clausole contenute in tale contratto costituiscano un'intesa che possa restringere in modo rilevante la concorrenza sul mercato, ai sensi dell'art. 101 T.F.U.E.[33]

In particolare, le criticità concorrenziali individuate nel provvedimento di avvio dell'istruttoria sono ravvisate in alcune clausole che appaiono esorbitare lo scopo di garantire la continuità aziendale delle imprese coinvolte nell'operazione, ed in particolare nelle pattuizioni aventi ad oggetto: (*i*) la previsione di un obbligo in capo a Tim di acquisto esclusivo dei servizi di accesso nei mercati all'ingrosso della durata di quindici anni, rinnovabili per ulteriori quindici anni; (*ii*) la clausola del prezzo di maggior favore, in base alla quale, nel caso FiberCop faccia offerte più convenienti ad altri operatori per gli stessi servizi di accesso venduti a Tim, nel periodo in cui il contratto è in vigore, tali condizioni devono essere applicate anche a Tim; (*iii*) il meccanismo di sconti a volume nel servizio di accesso attivo sulla rete in fibra, che prevede degli sconti in base al raggiungimento di determinate soglie individuate in base al rapporto tra linee attivabili e linee attivate.

A parere dell'Agcm, infatti, l'eccessiva durata della clausola di esclusiva, conclusa tra Tim, primo operatore nel mercato dei servizi al dettaglio, e Fibercop, leader nel mercato dei servizi di accesso all'ingrosso, produrrebbe l'effetto di assicurare a vantaggio di quest'ultima una larga parte (circa il 40%) della domanda dei servizi di

---

[31] Si vedano i parr. 33-35 della *Comunicazione sulle restrizioni*, cit.

[32] Agcm, provv. n. 3145 del 17 dicembre 2024, *I-874- Master service agreement Tim-Fibercop*.

[33] L'Agcm ha, infatti, ritenuto che l'accordo in questione ha effetto sui mercati dei servizi al dettaglio e all'ingrosso aventi la dimensione dell'intero territorio nazionale, e pertanto ha considerato ricorrente il pregiudizio al commercio tra gli Stati membri, presupposto questo per l'applicazione della normativa eurounitaria.

accesso all'ingrosso, con potenziali effetti escludenti nei confronti dei concorrenti presenti in tale mercato.

Rispetto, poi, agli sconti a volume l'Agcm ha rilevato che, sebbene le offerte siano teoricamente aperte anche ai concorrenti di Tim, tuttavia le soglie previste nel meccanismo degli sconti sono tali da poter essere raggiunte solo da quest'ultima, con possibili effetti escludenti nel mercato dei servizi di telefonia al dettaglio[34]. Inoltre, ha osservato che, attraverso la clausola del prezzo di maggior favore, Tim è in grado di assicurarsi un indebito vantaggio rispetto ai propri concorrenti, avendo sempre la garanzia di ottenere il minor costo di fornitura.

Proprio in ragione dell'avvio del procedimento, Fibercop e Tim hanno presentato, ai sensi dell'art. 14-*ter* della l. 287/90, gli impegni che, a parere delle parti dell'accordo, dovrebbero permettere il superamento delle criticità concorrenziali sopra individuate.

In particolare, è stata proposta una rimodulazione della durata della clausola di esclusiva per il solo servizio di accesso alla rete con tecnologia in fibra FTTH (ossia fino all'abitazione del cliente), per la quale è stata proposta una durata variabile nell'ambito di tre zone geografiche individuate in base ai livelli di sviluppo concorrenziale in essi raggiunti[35].

---

[34] L'Agcm ha, altresì, rilevato che il meccanismo degli sconti appare particolarmente pregiudizievole sotto il profilo concorrenziale, in quanto riguarda un tipo di accesso, ossia quello dell'accesso attivo di tipo VULA FTTH, nel quale è stato confermato l'obbligo dei prezzi orientati al costo, e non riguarda i servizi passivi (tipo G-pon e semiG-pon) nei quali è stato previsto un obbligo di prezzi equi e ragionevoli. Il meccanismo di sconti non incentiverebbe, allora, l'utilizzo dei servizi passivi di accesso nei quali si è sviluppata una forte presenza di Fastweb, e quindi potrebbe rafforzare ulteriormente l'effetto di *foreclosure* nei confronti dei concorrenti di Fibercop nei mercati dell'accesso all'ingrosso.

[35] Sono state distinti tre cluster: (*a*) il primo *cluster* costituito dalle aree oggetto di finanziamenti pubblici per la realizzazione della fibra, caratterizzata da una sola rete, con una quota di mercato di Open Fiber, pari al 70-75% e una quota di Fibercop del 25-30%; (*b*) il secondo *cluster* formato dalle aree c.d. nere, comprensive di circa 175 Comuni, in cui già sono presenti almeno due operatori detentori della rete, e dove l'esclusiva in favore di Fibercop vincola circa il 25% della quota di mercato dei servizi al dettaglio con accesso a banda larga e ultra larga; (*c*) il terzo *cluster* è formato dalle restanti aree in cui non è ancora iniziato lo sviluppo dell'accesso FTTH e che costituisce il 44% delle unità immobiliari nazionali.

In particolare, è stata proposta per le c.d. aree nere (*cluster* 2), maggiormente concorrenziali, una configurazione dell'obbligo di esclusiva in periodi successivi così caratterizzati: (*i*) un primo periodo di tre anni in cui Tim sarà obbligata ad acquistare i servizi di accesso alla rete in via esclusiva da Fibercop, che potrà fornire il servizio direttamente mediante la propria rete o indirettamente, utilizzando le infrastrutture dei concorrenti e svolgendo in tal caso solo una funzione di rivenditore; (*ii*) un successivo periodo della durata di dieci anni, in cui l'obbligo di esclusiva di Tim avrà ad oggetto solo gli accessi che Fibercop potrà fornire direttamente mediante la propria rete, con l'esito che per gli accessi che Fibercop non sarà in grado di coprire con la propria infrastruttura Tim avrà la facoltà di rifornirsi da altri operatori; (*iii*) un terzo ulteriore periodo di sei anni, in cui Tim dovrà garantire un livello di accessi pari a quelli acquistati da Fibercop al termine del periodo dei dieci anni precedenti.

Nel *cluster* 3, ossia quello in cui non è ancora iniziato il *roll-out* degli accessi in fibra FTTH, è stato proposto il medesimo meccanismo, con l'unica differenza che il periodo iniziale di esclusiva è di quattro anni, seguito poi dal secondo periodo di dieci anni in cui l'esclusiva è limitata agli accessi che Fibercop potrà fornire con la propria rete, e un ulteriore periodo di sei anni, caratterizzato dall'obbligo di Tim di mantenere per i sei anni successivi un livello di accessi sull'infrastruttura di Fibercop pari a quello raggiunto al termine del periodo precedente. Nel *cluster* 1, relativo alle aree oggetto di sussidi pubblici, vengono mantenuti gli obblighi di esclusiva di quindici anni rinnovabili per altri quindici, anche nella fornitura degli accessi in fibra con tecnologia FTTH.

Per quanto riguarda gli sconti a volume, si introduce un ulteriore set di sconti previsti per gli accessi passivi, oltre a quelli attivi già oggetto dell'accordo *MSA*, anch'essi peraltro concessi solo al raggiungimento di volumi di acquisto, e progressivamente più alti fino al raggiungimento dell'esclusiva.

Un ulteriore impegno presentato ha riguardato l'obbligo assunto da Tim di retrocedere a Fibercop i diritti di utilizzazione dei collegamenti in fibra (c.d. IRU) con i clienti *business* nel caso di intervenuta cessazione del rapporto prima della scadenza dei suddetti

diritti, in modo tale da permettere a Fibercop di concedere i diritti medesimi ad altri operatori che ne facciano richiesta e superare così problemi di ritenzione di capacità produttiva con finalità escludenti.

Nell'attesa della valutazione dell'Agcm sugli impegni presentati da Fibercop e Tim, possono formularsi alcune considerazioni sui possibili effetti pregiudizievoli per la concorrenza derivanti dalle clausole del *MSA*, e dagli impegni proposti.

Occorre, sul punto, precisare che si tratta di un'intesa verticale, in quanto conclusa tra imprese operanti in due livelli diversi della catena produttiva distributiva, e nel caso di specie riguardante l'impresa attualmente dominante nella fornitura all'ingrosso dei servizi di accesso alla rete (Fibercop) e l'impresa leader nei mercati dei servizi di telefonia fissa al dettaglio (Tim). Come noto, le intese verticali destano minori preoccupazioni in ordine ai possibili effetti restrittivi della concorrenza rispetto alle intese orizzontali, in quanto attuate tra imprese che non sono in concorrenza tra loro, e che si caratterizzano per il fatto che l'offerta dell'impresa a monte è parte della domanda dell'impresa a valle. Inoltre, in determinate circostanze possono generare delle efficienze in termini di riduzione del prezzo, di aumento della concorrenza non basata sul prezzo, di miglioramento della qualità dei servizi a vantaggio dei consumatori[36] (v. sul punto gli *Orientamenti sulla restrizioni verticali*[37], punti 12 e ss.).

Tali ragioni costituiscono il fondamento del regolamento generale concernente le intese verticali, che prevede un'esenzione dal di-

---

[36] Per l'evoluzione dell'approccio dell'antitrust europeo rispetto alle intese verticali v. M. Libertini, *Diritto della concorrenza dell'Unione europea*, Milano, 2014, p. 221 ss. La valutazione delle efficienze riconducibili alle intese verticali può ritenersi uno dei maggiori contributi che la scuola di Chicago, e l'analisi economica degli effetti delle condotte anticoncorrenziali, abbiano dato allo sviluppo del diritto antitrust europeo. Sul punto v. R.A. Posner, *Antitrust Law. An Economic Perspective*, Chicago, 1976; Id., *The rule of a reason and Economic Approach: Reflections on the Sylvania Decision*, in *University of Chicago Law Review*, Vol. 45, 1977; e del medesimo autore più recentemente Id., *Vertical Restraints and Antitrust Policy*, in *University of Chicago Law Review*, Vol. 72, 2005, p. 229 ss. Sull'influenza della scuola di Chicago sulla valutazione delle intese verticali v. C.S. Hemphill, *Posner on vertical restraints*, in *University of Chicago Law Review*, vol. 86, 2019, p. 1056 ss.

[37] Comunicazione della Commissione UE, *Orientamenti sulle restrizioni verticali*, (2022/C 248/01), del 30 giugno 2022.

vieto per tutti gli accordi verticali conclusi tra un fornitore e un acquirente, i quali non detengano una quota superiore al 30% rispettivamente nel mercato della fornitura e dell'acquisto del bene o servizio oggetto dell'accordo (art. 3 reg. 2022/270[38]), esenzione questa che viene meno laddove l'accordo contenga alcune tipologie di restrizioni considerate particolarmente gravi per il pregiudizio concorrenziale (come ad es. l'imposizione di un prezzo di rivendita).

Sebbene l'accordo di *MSA* non possa rientrare nell'esenzione, stante il superamento delle quote di mercato previste per la sua applicazione, è possibile utilizzare i criteri previsti nel reg. UE 20220/270 e negli *Orientamenti* della Commissione per valutare il possibile esito dell'istruttoria avviata dall'Agcm.

Se si considera, infatti, che il reg. 2022/720 individua come clausole particolarmente gravi, tanto da eliminare il beneficio dell'esenzione, le clausole di acquisto esclusivo di durata superiore a cinque anni, è ragionevole prevedere che la durata molto maggiore dell'obbligo di acquisto esclusivo imposto a Tim sarà considerata idonea a pregiudicare in modo sostanziale la concorrenza, effetto questo reso ancor più dannoso se valutato unitamente alle clausole di maggior favore e di sconti a volume[39]. Del resto, non pare che gli impegni proposti siano in grado di eliminare gli effetti di *foreclosure* tanto nel mercato dell'accesso all'ingrosso quanto nel mercato dei servizi al dettaglio.

Sul mercato dell'accesso, la durata dell'esclusiva appare ricalibrata soltanto rispetto al servizio di accesso in fibra FTTH nei cluster 2 e 3, rimanendo della durata trentennale nel *cluster* 1 ed altresì per tutti gli altri servizi. Peraltro, proprio nel *cluster* 1, concernente le aree sussidiate oggetto di finanziamento pubblico, è possibile os-

[38] Regolamento (UE) 2022/720 della Commissione del 10 maggio 2022 relativo all'applicazione dell'articolo 101, paragrafo 3, del Trattato sul funzionamento dell'Unione europea a categorie di accordi verticali e pratiche concordate. Per un commento sul nuovo regolamento v. P. MANZINI, *Le restrizioni verticali della concorrenza nel nuovo regolamento VBER*, in *Dir. comm. int.*, 2022, da p. 555; ed altresì P. GELATO e S. VERGANO, *Prime note a margine del Reg. Ue 720/22 e riflessi in materia di distribuzione selettiva*, in *Riv. dir. ind.*, 2022, da p. 90.

[39] Si veda l'art. 5, par. 1, lett. *a*), reg. UE 2022/720, nonché gli *Orientamenti sulle restrizioni verticali*, par. 247-249.

servare che, se è vero che attualmente l'operatore Open Fiber appare essere titolare della quota dominante nell'aggiudicazione delle gare per la realizzazione dell'infrastruttura in fibra, è altresì vero che l'esclusiva oggetto del *MSA* rischia di non rendere produttivi gli investimenti che verranno effettuati dall'aggiudicatore delle gare, laddove Fibercop decida di impegnarsi autonomamente nella realizzazione dell'infrastruttura nelle aree bianche, forte del fatto che in tal caso Tim avrà l'obbligo di acquistare i servizi di accesso in fibra da quest'ultima piuttosto che da Open Fiber per un periodo di tempo che potrà arrivare al trentennio[40].

Inoltre, andando a vedere nello specifico la rimodulazione della clausola di esclusiva proposta, può osservarsi in particolare che il periodo di esclusiva previsto è molto lungo (tredici o quattordici anni rispettivamente nel *cluster* 2 e 3), e sebbene nel secondo periodo di dieci anni riguarderà esclusivamente i servizi di accesso per i quali Fibercop potrà utilizzare la propria infrastruttura, ciò non permetterà di ridurre significativamente i livelli acquistati da Tim, anche in considerazione del meccanismo di sconti a volume, circostanza questa ulteriormente pregiudizievole in ragione del fatto che per ulteriori sei anni Tim dovrà assicurare il mantenimento dei medesimi quantitativi.

Anche rispetto agli effetti escludenti nei mercati dei servizi al dettaglio, gli impegni proposti non eliminano le criticità individuate dall'Agcm con riguardo agli sconti a volume, in quanto non fanno altro che estendere i medesimi problemi di raggiungibilità da parte degli altri operatori presenti nel mercato *retail* delle condizioni previste per gli sconti sui servizi di accesso attivo, anche su quelli di accesso passivo.

---

[40] Si consideri che con il provv. Agcm, *A-514-Condotte fibra Telecom Italia*, del 25 febbraio 2020, Telecom è stata sanzionata per aver posto in essere una strategia complessiva, che tra l'altro prevedeva, in relazione alle aree bianche, una condotta consistente nella realizzazione autonoma, rispetto ai soggetti aggiudicatari delle gare pubbliche, delle reti in fibra, e nell'attuazione di una strategia di cattura dei propri clienti nei servizi al dettaglio mediante la migrazione nelle reti di nuova generazione, con il rischio di impedire il configurarsi di forme di concorrenza infrastrutturale e sabotare, altresì, il piano di investimenti pubblici. La condotta abusiva è stata confermata anche dal Consiglio di Stato, che con sentenza del 13 novembre 2024, n. 9138, ha previsto soltanto la riduzione della sanzione.

Alla luce delle precedenti considerazioni, ed in mancanza di ulteriore revisione degli impegni proposti, appare ad oggi prevedibile un esito del procedimento che vieti l'accordo di *MSA* ai sensi dell'art. 101 del T.F.U.E.

## 6. *Prospettive concorrenziali nel mercato delle infrastrutture di rete fissa*

La cessione della rete Tim impone, in conclusione, una riflessione più generale su quelle che possono essere le prospettive future dello sviluppo concorrenziale del mercato relativo alle infrastrutture di rete fissa.

Infatti, se in un primo momento la dismissione volontaria della rete sembrava andare nella direzione della realizzazione in Italia di un'unica infrastruttura di rete fissa, peraltro posta sotto il controllo dello Stato, la vicenda ha indubbiamente incentivato la concorrenza infrastrutturale soprattutto tra operatori detentori delle reti di nuova generazione, che si caratterizzano, rispetto alle precedenti reti in rame, per non essere più esclusivo appannaggio del monopolista legale, potendo essere realizzate da qualunque impresa voglia investirvi. Inoltre, proprio perché le reti di nuova generazione costituiscono un importante veicolo di progresso economico, nonché di attuazione di diritti fondamentali della persona, la realizzazione delle infrastrutture di comunicazione elettronica per la fornitura di servizi è oggetto di programmi di finanziamenti pubblici, il che costituisce un'ulteriore leva alla concorrenza tra operatori detentori di una propria rete.

Sebbene, dunque, le reti di nuova generazione siano caratterizzate dalla maggiore facilità di creazione di nuove infrastrutture, occorre chiedersi che tipo di concorrenza potrà istaurarsi e se effettivamente potrà contribuire al miglioramento della tecnologia e della qualità delle reti[41].

Considerati, infatti, gli ingenti investimenti richiesti, nonché la necessità di superare numerosi ostacoli di natura amministrativa e

[41] Sui benefici che la concorrenza infrastrutturale nelle reti di nuova generazione potrà portare in termini di diminuzione di prezzi e qualità della rete, v. F. FLOREZ DUNCAN, R. ALIMONTI e S. SHARMA, *Sviluppo della concorrenza infrastrutturale*, cit., p. 353 ss.

tecnica per la realizzazione delle reti, il mercato sarà inevitabilmente caratterizzato dalla presenza di pochi operatori, con un elevato grado di concentrazione, potendosi, allora, qualificare come un oligopolio ristretto. Ciò, da un punto di vista concorrenziale, farà sì che, anche in assenza di una collusione tra le imprese, ci sarà un'interdipendenza strategica tra le condotte poste in essere dalle imprese, giacché il profitto realizzabile da un'impresa dovrà tener conto delle scelte in termini di prezzo e quantità attuate dalle altre imprese[42].

Il rischio che ne deriva è, allora, che, in assenza di alcun intervento regolatorio, i prezzi dei servizi di accesso potranno attestarsi a livelli molto più elevati, facendo conseguentemente aumentare il livello dei prezzi dei servizi *retail*.

In considerazione di tale potenziale effetto, il Body of European Regulators for Electronic Communications (Berec), in occasione dei lavori preparatori per l'emanazione del nuovo Codice europeo delle comunicazioni elettroniche, aveva proposto di estendere la nozione di impresa con significativo potere di mercato, fino a ricomprendervi anche il concetto di potere di mercato unilaterale (UPM), correlato ai contesti di mercato oligopolistici non collusivi[43].

Tale modifica avrebbe permesso di mantenere obblighi regolamentari non solo in presenza di una in posizione dominante, sin-

[42] La concorrenza nei mercati oligopolistici è stata considerata dai teorici dell'organizzazione industriale come esempio di una competizione strategica (gioco), in cui le imprese (giocatori) stabiliscono la propria strategia al fine di massimizzare il proprio profitto (vincita), tenendo conto, secondo una propria congettura, della strategia che i concorrenti adotteranno. Tale interpretazione è stata proposta soprattutto dai teorici dell'organizzazione industriale. La letteratura circa i modelli non cooperativi di concorrenza nell'oligopolio è vasta; tra i numerosi contributi, si rinvia per tutti a D.W. CARLTON, J.M. PERLOFF, *Organizzazione industriale*, III ed. italiana, Mc Graw Hill, Milano, 2012, p. 194 ss.; M. POLO, *Teoria dell'oligopolio*, Il Mulino, Bologna, 1993. Infatti, la reinterpretazione, da parte dell'organizzazione industriale, dei modelli economici dell'oligopolio non cooperativo alla luce della teoria dei giochi ha permesso di dimostrare come, nei mercati oligopolistici caratterizzati da determinate condizioni (i.e. grado di concentrazione elevato, barriere all'entrata, sostituibilità tra i prodotti delle imprese partecipanti alla concentrazione), la semplice interazione tra le imprese presenti nel mercato, in assenza di qualunque coordinamento tra le stesse, ha come effetto l'imposizione di prezzi più alti e/o una minore offerta rispetto alle condizioni di un mercato concorrenziale.

[43] BEREC, *Views on non-competitive oligopolies in the Electronic Communications Code*, BoR(17) 84.

gola o collettiva, bensì anche laddove le caratteristiche del mercato sarebbero state tali da incentivare l'attuazione di condotte unilaterali aventi un effetto peggiorativo dei parametri concorrenziali (i.e. prezzi, quantitità offerta, qualità e innovazione).

La proposta non ha trovato ad oggi accoglimento, tanto che negli *Orientamenti* della Commissione del 2018 l'esistenza di un oligopolio assume rilevanza solo nel caso in cui agevoli una collusione tra le imprese, situazione questa che viene ricondotta al concetto di significativo potere di mercato collettivo[44], ma non include il pregiudizio significativo alla concorrenza derivante da condotte unilaterali non coordinate che le imprese sono incentivate a porre in essere nei mercati oligopolistici ristretti.

L'evoluzione dei mercati delle infrastrutture verso un modello oligopolistico che non abbia le caratteristiche di funzionamento collusivo potrebbe, allora, indurre ad una revoca dell'intervento regolatorio *ex ante* con il rischio di un aumento dei prezzi di accesso, di riduzione degli investimenti nell'innovazione e nella qualità, a detrimento dei servizi forniti ai clienti finali.

Per evitare un tale esito appare, allora, auspicabile un ampliamento della nozione di significativo potere di mercato nella direzione proposta dal Berec, sì da includervi il potere di attuare comportamenti che costituiscano un *significativo ostacolo alla concorrenza*, in modo non dissimile da quanto previsto nel parametro di valutazione delle operazioni di concentrazioni adottato nell'art. 2 del reg. 139/2004, che, a differenza del test della dominanza previsto nel precedente reg. 4064/89, consente di valutare il peggioramento dell'equilibrio concorrenziale nei mercati oligopolistici non collusivi[45].

---

[44] Comunicazione della Commissione, del 7 maggio 2018, cit., par. 65 ss., in cui si specifica come il concetto di significativo potere di mercato collettivo deve essere interpretato sulla base dell'evoluzione del concetto di dominanza collettiva, che include i casi in cui più imprese si presentino congiuntamente attuando una strategia comune, sia in presenza di legami strutturali, sia in presenza di caratteristiche del mercato che siano tali da permettere nel lungo periodo di mantenere un coordinamento tacito.

[45] Sulle ragioni che hanno portato alla modifica del criterio di valutazione, v. Cfr. P. Cassinis, P. Saba, *La riforma comunitaria sul controllo delle concentrazioni*, in *Le nuove leggi civili commentate*, 2004, p. 405 ss.; A. Weitbrecht, *EU Merger Control in 2004 - An Overview*, in *E.C.L.R.*, 2005, 2, p. 67 ss.; Cfr. K. Fountoukakos, S. Ryan, *A*

Una tale modifica permetterebbe di fondare il mantenimento di un quadro regolatorio anche minimale, ad esempio attraverso l'imposizione di un obbligo di mantenimento di prezzi equi, non solo in presenza di una dominanza individuale o di un oligopolio collusivo, ma ogni qual volta le caratteristiche del mercato oligopolistico siano tali da determinare un peggioramento significativo dei parametri concorrenziali[46].

---

*new substantive test for UE merger control*, in *E.C.L.R.*, 2005, da p. 277 ss., p. 281; S. MAUDHUIT, T. SOAMES, *Changes in EU Merger Control: Part 2*, in *E.C.L.R.*, 2005, 2, p. 75. Che l'obiettivo della modifica fosse quello di permettere di valutare gli effetti anticoncorrenziali non coordinati in un mercato oligopolistico è reso esplicito dalla seconda parte del *considerando* 25, in cui si dichiara che la nozione di ostacolo significativo alla concorrenza effettiva dovrebbe essere interpretato come riguardante, al di là della creazione della posizione dominante, soltanto gli effetti non coordinati nei mercati oligopolistici. La questione dell'inadeguatezza del test della posizione dominante a valutare gli effetti anticoncorrenziali nei mercati oligopolistici non collusivi è stata analizzata con chiarezza e completezza da J. FINGLETON, D. NOLAN, *Mind the gap. La riforma del regolamento comunitario sulle concentrazioni*, trad. M. Brescia, in *Mercato concorrenza e regole*, 2003, p. 309 ss. Sulla valutazione degli effetti unilaterali negli oligopoli ristretti nell'operazione di concentrazione tra Telefonica e H3G nel mercato della telefonia mobile inglese, sia consentito il rinvio a S. SERAFINI, *Gli incerti confini del controllo sulle concentrazioni nei mercati oligopolistici non collusivi. Riflessioni a margine del caso Telefonica Europe/H3G UK*, in *Riv. dir. comm.*, 2020, da p. 591. Sull'estensione della nozione di significativo potere di mercato in modo da ricomprendervi il significativo ostacolo alla concorrenza assumono una posizione critica F. FLOREZ DUNCAN, R. ALIMONTI e S. SHARMA, *Sviluppo della concorrenza infrastrutturale*, cit., p. 365 ss.

[46] Sulla necessità di un'interpretazione tecnicamente orientata delle norme a tutela della concorrenza, ossia che tenga conto dell'evoluzione delle caratteristiche tecniche dei mercati, al fine di ampliare il significato delle nozioni tradizionali ed evitare gli effetti anticoncorrenziali riconducibili a caratteristiche tecniche nuove non immediatamente riconducibili all'applicazione tradizionale delle fattispecie *antitrust*, v. G. DE MINICO, *Unione, mercato e tecnica*, versione provvisoria della relazione al XL Convegno annuale dell'Associazione Italiana dei Costituzionali, *L'Unione Europea a confronto con la costituzione italiana*, pubblicata sul sito *https://www.associazionedeicostituzionalisti.it/images/convegniAnnualiAIC/2025_Torino/Giovanna_De_Minico.pdf*.

ALLEGRA CANEPA

# LA TUTELA DELLA CONCORRENZA IN EPOCA DI PIATTAFORME DIGITALI: UNA LETTURA SULL'EFFICACIA DELLA NORMATIVA ESISTENTE

SOMMARIO: 1. L'affermazione dell'economia digitale e dei c.d. ecosistemi. – 2. La tutela della concorrenza all'interno ed all'esterno dell'ecosistema: dal DMA alle linee guida sull'applicazione dell'art. 102 TFUE. – 3. Le acquisizioni quale "strumento" di creazione e consolidamento di un ecosistema e l'applicabilità della normativa europea sulle concentrazioni. – 4. Dal regolamento n. 1/2003 al DMA: una nuova evoluzione nei rapporti tra Commissione e autorità nazionali? – 5. Qualche considerazione conclusiva.

## 1. *L'affermazione dell'economia digitale e dei c.d. ecosistemi*

Con lo sviluppo tecnologico e l'affermazione della digitalizzazione, la struttura dei mercati ha subito profonde modifiche sia in relazione alla fisionomia degli operatori e dei servizi erogati che per quanto concerne le modalità di scambio. Tali trasformazioni hanno prodotto effetti sulle dinamiche di concorrenza e, proprio al fine di comprendere come queste si generino e se l'attuale quadro normativo possa considerarsi efficace, appare di interesse soffermarsi sulle piattaforme e, nello specifico, su quelle note come ecosistemi. L'utilizzo di questo termine appare particolarmente utile per descrivere l'assetto che questa tipologia di piattaforme riesce a creare attraverso una "politica espansiva" diretta all'aggregazione di servizi molto differenti tra di loro, sia regolamentati (come quelli finanziari[1]) sia non regolamentati (come l'ascolto della musica, il video

[1] Già la Comunicazione della Commissione del 24 settembre 2020 relativa a una Strategia in materia di finanza digitale per l'UE, COM(2020)591, al punto 6 sottoli-

streaming, ecc.), che consente di acquisire una posizione di forza sui mercati.

Prima di entrare nel dettaglio della struttura di questi operatori, può essere utile sottolineare come l'utilizzo del termine ecosistema per definirli non sia appannaggio della sola dottrina, delle autorità di regolazione e della giurisprudenza, ma anche della normativa. Infatti, il Regolamento 1925/2022 c.d. Digital Markets Act (DMA)[2], adottato proprio per limitare il condizionamento e il pregiudizio per il mercato che alcune piattaforme possono generare nel momento in cui raggiungono determinati parametri di fatturato e quantitativi (numero di utenti commerciali e finali che le utilizzano), fa riferimento a questo concetto[3]. Il regolamento menziona anche altri due

---

neava come i fornitori di servizi digitali fossero esclusi dall'applicazione della normativa e della vigilanza finanziaria.

[2] In tal senso si veda il Regolamento europeo n. 1925/2022 del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive UE 2019/1937 e Ue 2020/1828, in GUUE L265/1 del 12.10.2022 considerando n. 3 e n. 32.

Nella giurisprudenza, correlata a decisioni in materia antitrust, si veda ad esempio la sentenza della Corte di giustizia sulla decisione relativa al caso Google Alphabet nella quale si faceva riferimento all'ecosistema definendolo come un mercato multilaterale in grado di riunire diverse categorie di fornitori, clienti e consumatori che interagiscono con la piattaforma". Si tratta della sentenza della Corte di Giustizia del 14 settembre 2022, causa T-604/18, Google LLC e Alphabet, Inc v. Commissione, (Google Android case), p. 116.

[3] L'art. 3 co. 2 afferma che si presume che un'impresa sia un gatekeeper quando "raggiunge un fatturato annuo nell'Unione pari o superiore a 7,5 miliardi di EUR in ciascuno degli ultimi tre esercizi finanziari, o se la sua capitalizzazione di mercato media o il suo valore equo di mercato equivalente era quanto meno pari a 75 miliardi di EUR nell'ultimo esercizio finanziario, e se essa fornisce lo stesso servizio di piattaforma di base in almeno tre Stati membri; *b*) in relazione al paragrafo 1, lettera *b*), se fornisce un servizio di piattaforma di base che, nell'ultimo esercizio finanziario, annovera almeno 45 milioni di utenti finali attivi su base mensile, stabiliti o situati nell'Unione, e almeno 10000 utenti commerciali attivi su base annua stabiliti nell'Unione, identificati e calcolati conformemente alla metodologia e agli indicatori di cui all'allegato; *c*) in relazione al paragrafo 1, lettera *c*), se le soglie di cui alla lettera *b*) del presente paragrafo sono state raggiunte in ciascuno degli ultimi tre esercizi finanziari.

Sul tema tra gli altri A.C. Witt, *The Digital Markets Act - Regulating the Wild West*, in *Common Market Law Review*, 2023, p. 625 ss.; A. Reyna, *DMA and DSA Effective Enforcement - Key to Success*, in *Journal of Antitrust Enforcement*, 2024, p. 320 ss.; C. Brunetti, *I mercati digitali tra regolazione e concorrenza*, *Riv. orizz. dir. comm.*, 2024, p. 1081 ss.; D.M. Manescu, *Legislation Comment: Considerations on the Digital Markets Act, the Way to a Fair and Open Digital Environment*, in *European Business*

ulteriori aspetti caratterizzanti il processo di sviluppo di un ecosistema, e cioè lo sfruttamento di fattori strettamente tecnologici qualificanti i prodotti ed i servizi, ed organizzativi quali i legami contrattuali (e non solo) con operatori indipendenti presenti nel mercato di riferimento o in altri segmenti[4]. In realtà, anche l'esame di questi elementi è più complesso di quanto potrebbe apparire e richiederebbe la creazione di una tassonomia degli strumenti utilizzati per costruire e consolidare un ecosistema perché essi variano non solo a seconda della loro origine statunitense o cinese, ma anche a seconda della natura della piattaforma originatrice[5].

Se ad esempio consideriamo Amazon ed Apple, entrambe già identificate, ai sensi del procedimento previsto dal DMA, come gatekeeper, si nota come la prima ha basato il suo sviluppo funzionale sulla realizzazione di un marketplace attraverso accordi contrattuali con venditori inizialmente "esterni" e già operanti sul mercato; la seconda, Apple, sullo sviluppo di un sistema operativo applicato a vari dispositivi attraverso un'interoperabilità che si potrebbe definire "interna" perché garantita solo tra i device sviluppati dalla piattaforma originatrice. Ulteriori esempi in tal senso sono osservabili anche negli ecosistemi non di origine statunitense e realizzati da alcune piattaforme operanti sui mercati asiatici come l'ecosistema di Ant basato su un marketplace simile a quello di Amazon e quello

*Law Review*, 2024, p. 289 ss.; M. Orofino, *Il Digital Markets Act: una regolazione asimmetrica a cavallo tra diritto della protezione e diritto antitrust*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, p. 175 ss.

[4] Sul significato e sull'utilizzo di questo termine esiste una vasta letteratura, tra gli altri si vedano J. Moore, *Predators and Prey: A New Ecology of Competition*, *Harvard Business Review*, 1993, p. 75 ss.; J. Wareham, P. Fox, J.L. Cano Giner, *Technology ecosystem governance*, ESADE Working paper n. 225, January 2013; M.G. Jacobides, A. Gawer, C. Cennamo, *Towards a theory of ecosystems*, *Strategic Management Journal*, 2018, p. 2255 ss.; J. Rietveld, M.A. Schilling, C. Bellavitis, *Platform strategy: managing ecosystem value through selective promotion of complements*, *Organization Science*, 2019, p. 1125 ss.; P. Hornung, *The Ecosystem Concept, the DMA, and Section 19a GWB*, *Journal of Antitrust Enforcement*, vol. 12, 2024, p. 396 ss.

[5] Per un'analisi di dettaglio sul punto si veda L. Zhang, *When platform capitalism meets petty capitalism in China: Alibaba and an integrated approach to platformization,* in *Intern. Journ. Comm.*, 2020, p. 114 ss. e A. Canepa, *Dai dati al denaro. Come le piattaforme sono diventate ecosistemi dagli Stati Uniti alla Cina*, in L. Ammannati, A. Canepa (a cura di), *Tech Law. Il diritto di fronte alle nuove tecnologie*, Editoriale Scientifica, Napoli, 2021, p. 227 ss.

di WeChat, originato da una piattaforma di social media che ha avuto uno sviluppo estremamente rapido proprio grazie al "fattore tecnologico". Quest'ultimo consente di osservare una variante sul piano tecnologico rispetto a quello di Apple perché consentiva anche l'integrazione di app esterne e di nuove funzionalità attraverso l'introduzione di modifiche dell'esistente al fine di garantire l'offerta più ampia possibile di beni e servizi[6]. In tal modo, quanto realizzato risultava già automaticamente integrato nell'ecosistema e questo ha portato ad una stima del numero di servizi o funzionalità attualmente già collegati superiore complessivamente ai 4,3 milioni[7]. In questo caso, la possibilità di modifica, oltre che di integrazione, risulta particolarmente attrattiva per gli operatori, favorendo il loro collegamento in qualità di *complementors*[8].

Allo stesso tempo un accesso immediato e unico ad una gamma così ampia di beni o servizi, sistema definibile "*one-stop-shopping*"[9], permette agli utenti finali una semplificazione e velocizzazione del processo di acquisto perché l'utente è accompagnato e indirizzato nella scelta grazie ad un'accurata profilazione e predizione delle preferenze degli utenti tramite algoritmi costantemente alimentati da nuovi dati per risultare sempre più performanti. Del resto, la capacità di anticipare i desideri dei consumatori e la soddi-

---

[6] Per una ricostruzione storica di questo percorso si veda J. Webb Q. Yang, *China's Tencent becomes an investment powerhouse, using deals to expand its empire*, 2021, *Wall Street Journal*, *www.wsj.com*.; G. Goggin, *Apps: from mobile phones to digital lives*, Wiley, 2021; J. Lianrui, D.B. Nieborg, T. Poell, *On super apps and app stores: digital media logics in China's app economy*, in *Media Culture & Society*, 2022, p. 1437 ss. Sullo sfruttamento delle potenzialità *open source* offerte da Android rispetto ad altri sistemi operativi alla base dei servizi offerti dalle diverse piattaforme si veda in particolare K. Jia, M. Kenney, *The Chinese Platform Business Group: An Alternative to the Silicon Valley Model?*, in *Journ. Chinese Gov.*, 2021 e rep. anche sul sito *www.ssrn.com*.

[7] Su questo dato si veda in particolare WeChat Statistics and User Trends for China in 2025, *https://marketingtochina.com/wechat-statistics/*.

[8] Per un approfondimento di questo termine si veda in particolare H. Li, W.J. Kettinger, *Building blocks of software platforms: understanding the past to forge the future*, *Journ. Ass. Inform. System*, 2020.

[9] Sull'efficacia del "one-stop-shopping" si veda in particolare A.V. Ertemel, M.L. Civelek, *Analyzing the Effect of One-Stop Shopping on Purchase Intention in E-Commerce*, *Intern. Journ. Information Systems in Service Sector*, 2022, p. 1 ss.; M. Rigel, *One-Stop-Shopping hinders Specialization*, Collaborative Research Center Transeregio, German Research Foundation, Discussion Paper n. 701/2025, *https://www.crctr224.de/research/discussion-papers/archive/dp701*.

sfazione generata da un'offerta personalizzata riducono l'interesse a ricercare altre offerte e spingono a concludere gli acquisti senza neppure valutare l'offerta di altri operatori[10].

Una volta attuata la scelta, l'utente finale può anche condurla a termine senza dover abbandonare la piattaforma grazie anche all'integrazione, tra i servizi offerti, di quelli di pagamento e di accesso semplificato al credito, come il Buy Now Pay Later[11], capaci di realizzare un completo lock-in dell'utente che non ha più bisogno di ricercare nessun bene o servizio al di fuori dell'ecosistema[12].

Un simile assetto, difficilmente replicabile dagli operatori esterni all'ecosistema, prevede l'offerta di servizi finanziari, attraverso una particolare tipologia contrattuale, non pienamente rispondente a quelle "tradizionali"[13], sulla base della quale gli istituti finanziari rimangono a tutti gli effetti i prestatori del servizio di pagamento sia per quanto concerne "l'infrastruttura" che il conto corrente[14].

---

[10] Va ricordato come la teoria del consumer choice approach individui nella libertà di scelta del consumatore un elemento centrale per il diritto della concorrenza perché funzionale proprio al raggiungimento dell'efficienza del mercato. Sul punto si veda in particolare AVERITT, LANDE, *Consumer sovereignty: a unified theory of antitrust consumer protection law*, in *Antitrust Law Journal*, 1997, p. 713 ss. e ID., *Using the Consumer choice approach to antitrust law*, in *ibidem*, 2007, p. 175 ss.

[11] Per un approfondimento sulle caratteristiche di questo servizio e sulla rilevanza specifica negli ecosistemi si consenta il rinvio a A. CANEPA, *Big Tech e mercati finanziari: "sbarco pacifico" o "invasione"? Analisi di un "approdo" con offerta "à la carte"*, in *Riv. trim. dir. ec.*, 2021, 3, p. 465 ss. e ID., *Super Apps, pagamenti mobile e nuove forme di credito digitale al consumo: il Buy Now Pay Later*, in L. AMMANNATI, A. CANEPA (a cura di), *La finanza nell'età degli algoritmi*, 2023, p. 95 ss.

[12] Il lock-in risulta ancora più efficace se si considerano le c.d. Super App nelle quali si garantisce la visualizzazione ed il pagamento mediante subapplicazioni, c.d. mini-programmi con funzionalità simili a quelle di una app ed alle quali si accede senza *download* perché è sufficiente il QR Code.

[13] Secondo Resano potrebbe essere vista come una combinazione di caratteristiche riconducibili ad un contratto di agenzia e di *outsourcing.* e che, come tale, andrebbe qualificata come una nuova tipologia. Si veda J.R. MARTINEZ RESANO, *Regulating for competition with Big Techs: banking-as-a-service and beyond banking*, 2021, rep. sul sito *www.sssrn.com*. Sul punto l'EBA aveva sottolineato come, in alcuni casi, i servizi potrebbero essere considerati di natura tecnica con conseguente esclusione anche dal perimetro di supervisione. Si veda l'Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06, p. 87.

[14] Proprio in relazione a questo particolare schema in rapporto alla tutela dell'utente l'EBA ha evidenziato la possibile necessità di verificare casi specifici nei quali

La realizzazione di un sistema di questo tipo, *multi-actor* o *multi-product*, genera effetti sugli operatori presenti sul mercato sia preliminarmente, affinché entrino a far parte dell'ecosistema, sia successivamente, in quanto impone agli aderenti delle "regole di permanenza" (basti pensare ai rating di gradimento solo per fare un esempio)[15], in quanto il mancato soddisfacimento da luogo all'immediata esclusione. Le implicazioni concorrenziali derivanti dall'assetto descritto inizialmente non sono state percepite nel loro complesso tanto che in Cina, lo sviluppo di modalità di pagamento da integrare nell'ecosistema è stata inizialmente addirittura incentivata con alcuni interventi normativi per favorire una maggiore inclusione finanziaria, uno sviluppo economico più rapido e per motivi di strategia geopolitica e di rafforzamento nello scenario globale[16]. Successivamente, però, anche in Cina sono state adottate azioni dirette a contrastare la rilevanza assunta da queste piattaforme sul mercato anche attraverso l'imposizione di separazioni societarie[17].

---

la prestazione di servizi possa avere una differente qualificazione e sia caratterizzata da una scarsa trasparenza sui ruoli degli operatori coinvolti e sul soggetto autorizzato. Nello specifico si precisa che può essere necessario valutare se una determinata prestazione di servizi rientri nell'ambito di un contratto di agenzia, di un accordo di esternalizzazione o necessiti di autorizzazione. Si veda il documento dell'European Banking Authority, Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06, p. 91.

[15] Sul punto si vedano in particolare A. Zoppini, *Le domande che ci propone l'economia comportamentale ovvero il crepuscolo del "buon padre di famiglia"*, in Rojas Elgueta, N. Vardi (a cura di), *Oltre il soggetto razionale*, Roma University Press, 2014, p. 11 e Natoli, *Il diritto privato regolatorio*, in *Riv. Regolazione dei mercati*, n. 1/2020, *www.rivistadellaregolazionedeimercati*.

[16] Su quest'aspetto, in particolare, S. Rolf e S. Schindler utilizzano l'espressione "State platform capitalism". Si veda *The US-China rivalry and the emergence of state platform capitalism*, in *Environment and Planning: a Economy and Space*, 55(5), p. 1255.

[17] Nel 2021 alla piattaforma Ant è stata preliminarmente negata la quotazione in borsa e successivamente è stata imposta dal governo una separazione societaria. Va ricordato che contestualmente vi è stata un'azione regolatoria diretta a ridurre la capacità di sfruttamento dei dati attraverso l'introduzione del China Personal Information Protection Law (PILP) e del Provisions on the Management of Algorithmic Recommendations in Internet Information Services entrato in vigore nel 2022. Sul punto in particolare J.M. Fried, E. Kamar, *Alibaba: a case study of synthetic control*, *Law Working Paper*, n. 533/2020; D. Albrect, *The Internet Information Services Algorithm*

Nello scenario europeo, nel quale nessuna delle c.d. Big Tech si è sviluppata[18], ben prima dell'affermazione del mercato digitale, la Commissione, seppur con riferimento al modello di impresa verticalmente integrata non pienamente equiparabile, aveva evidenziato, come in presenza di una maggioranza di simili imprese operanti in un determinato settore, i potenziali interessati ad entrare in quel segmento di mercato avessero necessità di maggiori risorse finanziarie per riuscire ad entrare visti i vantaggi replicabili soltanto da altre imprese integrate in maniera analoga[19].

Pertanto, gli ecosistemi di origine statunitense, come sarà evidenziato, sono stati oggetto negli anni di indagini antitrust sotto differenti profili, in particolare l'abuso di posizione dominante, con applicazione di sanzioni economiche, seppur dopo l'espletamento di procedimenti lunghi e complessi.

Anche per questo sia il documento di Impact Assessment che il DMA stesso, avevano evidenziato la necessità di disporre di misure specifiche, capaci di intervenire anche *ex-ante*, tenuto conto che questi ecosistemi "esercitano un controllo su interi ecosistemi di piattaforme nell'economia digitale e per gli operatori di mercato esistenti o nuovi è estremamente difficile, a livello strutturale, sfidarle o contrastarle, indipendentemente dal loro livello di innovazione[20] o efficienza. La contendibilità è ridotta in particolare a causa dell'esistenza di barriere molto alte all'ingresso o all'uscita"[21].

---

*Recommendation Management (IISARM) Regulations in China*, *Computer Law Review International*, 2022, p. 97 ss.

[18] L'unico gatekeeper "europeo" designato dalla Commissione ai sensi del DMA nel 2024 è Booking.

[19] Si veda in particolare la Decisione della Commissione, caso AT.39523 - Slovak Telekom, del 15 ottobre 2014, considerando 291. Sull'assimilabilità dei comportamenti delle imprese verticalmente integrate con le piattaforme dotate di ecosistemi si veda in particolare J. Padilla, J. Perkins, & S. Piccolo, *Self-Preferencing in Markets with Vertically Integrated Gatekeeper Platforms*. *The Journal of Industrial Economics*, 70, 2022, p. 371 ss.

[20] Quest'ultima intesa, come complementare ad equità e contendibilità, è più volte richiamata in sede di considerando (v. i 3, 4, 17, 25, 32, 33, 57, 59).

[21] Considerando 3 del DMA. Nell'Inception Impact Assessment, *Digital Services Act package: ex ante regulatory instrument for large online platforms with significant network effects acting as gatekeepers in the European Union's internal market*, (2020)2877647, giugno 2020, si metteva in luce come "a small number of large online

La possibilità di un intervento *ex ante* può consentire di agire preventivamente sull'adozione di comportamenti capaci di creare squilibri profondi tra gli operatori, non limitando l'azione al solo momento nel quale gli effetti si sono già prodotti, come previsto per l'accertamento delle condotte anticoncorrenziali[22]. Quest'ultimo aspetto merita particolare attenzione, visto che il modello di business degli ecosistemi appare pensato fin dalla loro costituzione non tanto per garantirgli di essere concorrenziali sui mercati, bensì per fargli acquisire una posizione di forza sul mercato e ridurre quanto più possibile qualunque tipologia di concorrenza non solo all'esterno ma anche all'interno di un ecosistema.

Per comprendere se l'assetto delineato possa essere considerato tale da garantire un'integrazione priva di sovrapposizioni e un incremento di efficacia, può essere utile soffermarsi sulle previsioni del DMA non solo sul piano contenutistico e regolatorio[23], ma anche in rapporto all'assetto di competenze che delinea tra autorità nazionali e Commissione.

## 2. *La tutela della concorrenza all'interno ed all'esterno dell'ecosistema: dal DMA alle linee guida sull'applicazione dell'art. 102 TFUE*

Il DMA, come anticipato, ha quale focus l'intervento sulle grandi piattaforme nonché i gestori di servizi digitali o "core

---

platforms increasingly determines the parameters for future innovations, consumer choice and competition".

[22] Sul punto G. De Minico sottolinea come "Con il vento nuovo cambia la missione del costituzionalismo economico, non più promuovere la competition verso l'altro – mimando ideali piazze competitive rivelatesi poi non promettenti per i nuovi entranti – ma imbrigliare, catturare il potere digitale delle Autorità private per consentire ai terzi di contestarne l'indebita dominanza". Si veda G. De Minico, *Nuove tecniche per nuove diseguaglianze. Case law: disciplina delle telecomunicazioni, Digital Service Act e neurodiritti*, in *federalismi*, n. 6/2024, p. 15.

[23] Per un focus sulla discussione esistente al riguardo si veda in particolare R. Podszun, P. Bongartz and S. Langenstein, *The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers*, *Journal of European Consumer and Market Law*, 2021, p. 60 ss.

platform services"[24] capaci di dare luogo a scarsa contendibilità e iniquità sul mercato. L'azione nei confronti di questi soggetti qualificati come gatekeepers è articolata nell'imposizione di obblighi, finalizzati al perseguimento di obiettivi di contendibilità, equità ed innovazione, a carico di quelle piattaforme che, a seguito di una procedura di designazione, avviatasi nel maggio del 2023, dispongono dei parametri quantitativi previsti per la qualificazione come gatekeeper. Si ha, cioè, un'identificazione presuntiva sulla base dei parametri indicati, accompagnata da un obbligo per gli operatori interessati di fornire informazioni che però non rappresenta automaticamente un'autodichiarazione di essere qualificabili come gatekeeper perché questo avviene solo con l'adozione della decisione della Commissione.

Le misure introdotte sono pensate per influire sulle differenti fonti di alimentazione, tra loro correlate, ed in particolare sulla contestuale capacità di influenza sulle scelte degli utenti e sull'autonomia degli utenti commerciali. Infatti, il quadro delle tecniche utilizzate da queste piattaforme comprende sia quelle per la realizzazione di un ecosistema che quelle per il suo consolidamento, anch'esse capaci di creare squilibri concorrenziali all'interno del marketplace. Tra di esse in questa sede si è scelto di esaminarne due in modo specifico in quanto rilevanti nella formazione e nel consolidamento dell'ecosistema e tali da consentire anche di valutare come il DMA e la disciplina della concorrenza potrebbero agire.

La prima condotta identificata come autopreferenza svolge un ruolo importante nel consolidamento e rafforzamento dell'ecosi-

[24] Ai sensi del DMA, nello specifico dell'art. 3 co. 3, se una piattaforma raggiunge tutte le soglie quantitative già richiamate (sulle quali si veda la nota 3), deve notificare tale informazione alla Commissione senza indugio. Sulla base di questa previsione, il 6 settembre 2023 risultavano designati come gatekeepers soggetti, pertanto, agli obblighi del DMA, Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft, ai quali il 12 marzo 2024 si è aggiunto Booking. Va evidenziato come il caso di ByteDance sia stato anche oggetto di una causa di fronte alla Corte di Giustizia in quanto la piattaforma aveva impugnato il provvedimento della Commissione relativo al suo inserimento tra i gatekeepers. Si veda la Sentenza della Corte di Giustizia del 17 luglio 2024, Bytedance c. Commissione, causa T-1077/23, ECLI:EU:T:2024:478.

Core platform services (CPS) ai sensi dell'art. 2 co. 2 del DMA possono essere considerati i servizi di intermediazione online, motori di ricerca online, servizi di rete o sistemi operativi.

stema e, proprio per questo, è stata oggetto di numerosi procedimenti avviati dalla Commissione ai sensi dell'art. 102 TFUE, conclusi con l'applicazione di sanzioni ed è stata anche espressamente disciplinata dal DMA. La seconda concerne il ricorso alle acquisizioni, intese come singole operazioni aventi ad oggetto altre imprese, spesso operanti in segmenti di mercato differenti da quelli di operatività della piattaforma. Queste sono state utilizzate, insieme agli accordi contrattuali, per costituire l'ecosistema ed in alcuni casi anche rafforzarlo, ampliando i segmenti di mercato di operatività ed eliminando dal mercato potenziali concorrenti. Come sarà evidenziato, vi sono state anche acquisizioni di piccole imprese ed in particolare start-up per la loro strategicità nel rafforzamento di un'offerta sempre più innovativa, oltre che differenziata.

L'autopreferenza può essere definita come una situazione nella quale la piattaforma sfrutta gli algoritmi ed i dati raccolti, direttamente ed indirettamente attraverso i componenti del suo ecosistema, al fine di indirizzare gli utenti verso i propri prodotti. Nella bozza di linee guida relative all'applicazione dell'art. 102 TFUE sull'abuso di posizione dominante, attualmente in discussione[25], questa condotta viene qualificata con il termine "autoagevolazione" ed identificata in modo puntuale come comportamento attivo diretto a concedere un trattamento preferenziale ai propri prodotti[26] da ritenere abusivo quando si discosti dalla concorrenza basata sui meriti e produca effetti di esclusione della concorrenza.

Nello specifico, quest'ultima può essere realizzata attraverso un posizionamento o un'esposizione del prodotto[27] funzionali ad

---

[25] Comunicazione della Commissione, Linee direttrici sull'applicazione dell'articolo 102 del Trattato sul funzionamento dell'Unione europea al comportamento abusivo delle imprese dominanti volto all'esclusione della concorrenza, 2024, p. 4.3.3.

[26] Si veda in tal senso anche la sentenza del Tribunale del 10 novembre 2021, Google e Alphabet/Commissione (Google Shopping), causa T-612/17, punto 240.

[27] Sulla rilevanza del posizionamento si veda in particolare J. Fong, O.R. Natan, R. Pantle, *Consumer Inferences from Product Rankings: The Role of Beliefs in Search Behavior*, luglio 2025, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896993*; con riferimento al posizionamento e la rilevanza sui meccanismi di asta si consenta il rinvio a A. Canepa, *NFTs, Gamification e utilità correlate. Andamento del mercato tra diminuzione dell'interesse al possesso ed incremento di valore dell'accesso* in A. Canepa (a cura di), *Il mercato dei Non fungible Tokens tra arte, moda e gamification*, Milano University Press, 2024, p. 23 ss.

una manipolazione del comportamento e delle scelte degli utenti non solo negli acquisti ma anche nelle vendite in asta su piattaforma.

Tra gli esempi utili per analizzare più nel dettaglio questa condotta vi è Amazon ed il suo marketplace. Quest'ultimo commercializza prodotti a marchio Amazon e molti altri di venditori collegati contrattualmente alla piattaforma. Il contratto sottoscritto spesso non è frutto di una scelta pienamente libera di questi operatori perché rimanere esterni all'ecosistema garantisce una visibilità molto minore nei confronti degli utenti con tutte le implicazioni che ne conseguono non soltanto sulla possibilità di risultare concorrenziali ma anche di essere messi fuori mercato. Da questo punto di vista le due parti non possono essere considerate in posizione paritaria, bensì in una situazione qualificabile come una dipendenza economica. In tal senso è utile ricordare come, ad esempio, il contratto di Business Solution del servizio "vendere su Amazon" avesse, tra le altre, una previsione di necessaria parità di condizioni che il venditore doveva mantenere tra i prodotti proposti sul marketplace e quelli su altri canali di vendita in modo che questi ultimi non potessero risultare maggiormente concorrenziali[28].

Ciò che però risulta più significativo ai fini dell'individuazione dell'autopreferenza è proprio l'utilizzo dei dati di vendita raccolti dagli utenti commerciali operanti nel marketplace e la loro automatica integrazione nel set di dati utilizzato dall'algoritmo. In questo modo Amazon otteneva un duplice vantaggio, e cioè una profilazione più accurata e la capacità di calibrare le sue offerte assumendo decisioni aziendali strategiche, quali la vendita di prodotti equivalenti a quelli più venduti con il marchio Amazon. Peraltro, la piattaforma, sfruttando la propria logistica, poteva garantire anche prezzi, comprensivi di servizi accessori, come la spedizione, inferiori o identici. In questo modo i consumatori venivano indirizzati

[28] Il venditore era libero di determinare quali prodotti offrire sul *marketplace* di Amazon ma era obbligato a mantenere la parità tra i prodotti offerti tramite gli altri canali di vendita e i prodotti che immetteva nel catalogo di Amazon con riguardo, in particolare, alle condizioni e ai termini del servizio di assistenza garantite sui prodotti offerti nonché alle "informazioni necessarie", così come definite nel contratto di "Business Solutions".

sempre di più verso i prodotti a marchio Amazon, costringendo gli altri utenti commerciali presenti nel marketplace a rivedere i loro prezzi per cercare di rimanere competitivi e posizionati tra i primi risultati di ricerca[29].

Pur a queste condizioni, difficilmente un operatore prendeva in considerazione come opzione l'abbandono del marketplace, in quanto avrebbe perso gran parte della sua visibilità nonché degli utenti ormai fidelizzati da Amazon, tenuto conto che i dati dei consumatori che hanno acquistato i suoi prodotti sono nella disponibilità della sola piattaforma. Ciò significa l'esistenza di entrambi i requisiti che escludono la contendibilità del mercato, e cioè l'assenza di barriere all'ingresso e la presenza di costi di uscita[30].

Non va dimenticato che, oltre agli aspetti concorrenziali richiamati, vi possono essere ulteriori ripercussioni negative per il consumatore. Infatti, quest'ultimo, anche qualora fosse disposto a pagare il prezzo esposto, fattore che potrebbe consentire il superamento dell'iniquità[31], potrebbe comunque trovarsi a concludere

---

[29] Su questo aspetto specifico si consenta il rinvio a A. Canepa, *Alla ricerca dell'autonomia negoziale "perduta". Consumatori e venditori in epoca di profilazione e algoritmi*, in L. Ammannati, A. Canepa, G. Greco. U. Minneci (a cura di), *Algoritmi, Big Data, piattaforme digitali. La regolazione dei mercati in trasformazione*, Torino, Giappichelli, 2021, p. 155 ss.

[30] Sul punto è utile richiamare la teoria economica di Baumol anche se in essa, differentemente da quanto previsto nel DMA, si giustifica una maggiore concentrazione del mercato sulla base del potenziale ingresso a breve termine di imprese e del fatto che gli operatori storici possono essere sostituiti in futuro. Si veda W.J. Baumol, *Contestable markets: An uprising in the theory of industry structure*, in *American Economic Review*, 72(1), 1982, 1 ss. Sull'ampia discussione del termine contestabilità nel DMA ancor prima che il testo fosse approvato si vedano in particolare H. Schweitzer, *The Art to make Gatekeeper Positions Contestable and the Challenge to Know What is Fair: A Discussion of the Digital Markets Act Proposal*, Zeitschrift für europäisches Privatrecht, 2021 p. 503; Jacques Cremer *et al.*, *Fairness and Contestability in the Digital Markets Act*, *Yale Journal on Regulation*, 2023, p. 975 ss.

[31] Più in generale sul concetto di iniquità inteso anche come sproporzione esistente fra il prezzo realmente applicato e il valore economico complessivo dei prodotti ha avuto modo di pronunciarsi più volte la Corte di Giustizia. Si vedano in particolare le sentenze della Corte di Giustizia United Brands Company e United Brands Continental c. Commissione, causa C-27/76, del 14 febbraio 1978; sentenza British Leyland Public Limited Company c. Commissione, C-226/84, dell'11 novembre 1986; sentenza Kanal 5 Ltd e TV 4 AB c. Föreningen Svenska Tonsättares Internationella Musikbyrå (STIM) upa, causa C-52/07, dell'11 dicembre 2008 e sentenza, Ochranný svaz

l'acquisto ad una cifra maggiore di quella che il venditore avrebbe potuto fissare se avesse potuto decidere in autonomia[32].

Per questi motivi la Commissione aveva avviato un'indagine su questo comportamento già nel luglio 2019, seguita dalla comunicazione degli addebiti nel novembre 2020. A questa era stata poi collegata una seconda indagine, conclusasi con impegni volontari[33], riguardante anche il meccanismo di inserimento delle offerte dei venditori esterni nella c.d. Buy Box, una "corsia rapida di acquisto" per evidenziare l'offerta migliore su quel prodotto e diretta ad escludere tutte le altre opzioni ed informazioni, compresa l'indicazione del venditore[34]. Il sistema garantiva una corsia preferenziale ai prodotti a marchio Amazon, visto che l'algoritmo per inserire un

---

autorský pro práva k dílům hudebním o. s. (OSA) del 28 marzo 2014, causa C-351/12,; tutte rep. sul sito della Corte.

Va ricordato come anche la percezione di iniquità di un prezzo possa subire variazioni nel tempo e ridursi fino quasi ad azzerarsi. Sul punto si veda in particolare Xia, Monroe, Cox, *The Price is Unfair! A Conceptual Framework of Price Fairness Perceptions*, in «Journal of Marketing», 2004, p. 6 e ss.; L. Arnaudo, R. Pardolesi, Sul giusto prezzo tra Aquino e Aspen, in Merc. conc. Reg., 2016, p. 479 ss.; M. D'errico, *Unfair pracing e abuso di regolamentazione: il caso Aspen*, in Concorrenza e Mercato, 2017, p. 457 ss.

[32] Sul punto si veda in particolare A. Fletcher, Peter L. Ormosi, R. Savani, *Recommender Systems and Supplier Competition on Platforms*, *Journal of Competition Law & Economics*, Volume 19, Issue 3, September 2023, p. 397 ss.

[33] Si vedano le Decisioni della Commissione europea entrambe del 2° dicembre 2022, dei casi AT.40462 e 40703 entrambe reperibili su *https://competition-cases.ec.europa.eu/search?search=amazon&sortField=relevance&sortOrder=DESC*.

[34] Va segnalato come il sistema sia costruito per garantire una corsia preferenziale ai prodotti a marchio Amazon, visto che valuta prezzo, rispondenza al bene ricercato nonché logistica offerta. Ciò significa che i prodotti Amazon accompagnati dalla previsione di spese gratuite e spedizione molto rapida hanno le maggiori possibilità di "vincere la *buybox*", cioè, essere inseriti nella finestra di acquisto immediato, seguono i prodotti di venditori "esterni" che utilizzano la logistica Amazon e infine i prodotti di venditori terzi che gestiscono in proprio la logistica. L'identità del venditore diventa nota solo se il consumatore decide di fare un approfondimento e utilizzare l'opzione per visualizzarla. Proprio questo meccanismo insieme ad altri è stato individuato come una delle modalità di realizzazione di autopreferenza come evidenziato anche nelle indagini avviate in alcuni paesi europei come nel caso del *Bundeskartellamt* rif. B2-88/18, Amazon *online sales*, 17 July 2019. Sulla rilevanza della logistica in questo caso si veda in particolare J.S. Gans, P. Andreoli Versbach, Interplay Between Amazon Store and Logistics, settembre 2023, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4568024*.

prodotto nella Buybox valutava prezzo, rispondenza della proposta col bene ricercato nonché logistica offerta. Ciò significava che i prodotti a marchio Amazon caratterizzati dalla previsione di spese gratuite e consegna rapida avevano maggiori possibilità di "vincere la *buybox*" ed essere inseriti nella finestra di acquisto immediato; subito dopo, in ordine di possibilità di vincita, vi erano i prodotti di venditori "esterni" utilizzatori della logistica Amazon e, infine, i prodotti di venditori terzi che gestivano in proprio la logistica[35]. Una simile condotta è stata identificata come lesiva della concorrenza dalla Commissione che l'ha esaminata in due differenti casi, uno avente ad oggetto il marketplace ed uno la Buybox[36].

Questa fattispecie[37] è stata esplicitamente prevista dal DMA, già in sede di considerando[38], e qualificata come forma di tratta-

[35] In realtà, secondo alcuni autori, non in tutti i paesi la buybox avrebbe la stessa "impostazione di autopreferenza" e le differenziazioni sarebbero collegate anche alle regole esistenti. Sul punto si veda in particolare K.H. Lee, L. Musollf, *Entry Into Two-Sided Markets Shaped By Platform-Guided Search*, 19 maggio 2025, *https://economics.yale.edu/sites/default/files/jmp_entry_into_two-sided_markets_shaped_by_platform-guided.pdf* e F. Dendorfer, R. Seibel, What's In the Box? The Effect of Self-Preferencing on Amazon, 2025, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5219585*.

[36] Si tratta nello specifico delle Decisioni AT40463 e AT40703 entrambe del 20 dicembre 2022.

[37] La Commissione ha cominciato a valutare questo comportamento e le sue implicazioni con il Regolamento n. 1150/2019 introducendo disposizioni per garantire in primo luogo chiarezza e trasparenza nei rapporti in particolare per quanto concerne la comprensibilità delle informazioni su termini e condizioni della relazione. Uno specifico riferimento riguarda anche il posizionamento nelle ricerche e la trasparenza sui criteri utilizzati. La necessità di intervenire su questo tipo di condotta è presente anche nella proposta del Digital Markets Act specificamente dedicata alle piattaforme che svolgono un ruolo di gatekeeper. In dottrina con particolare riferimento al caso Amazon si vedano tra gli altri L. Khan, *Amazon's Antitrust Paradox*, *Yale Law Journ.*, 2017, p. 564 ss.; F. Etro, *Product selection in online markets*, Disei Working Paper n. 20/2020, *https://www.disei.unifi.it/upload/sub/pubblicazioni/repec/pdf/wp20_2020.pdf* e A Hagiu, T. The, J. Wright, *Should Platforms Be Allowed to Sell on Their Own Marketplaces?*, *Rand Journal of Economics, RAND Corporation*, vol. 53(2), p. 297 ss.

[38] Si tratta del considerando 52 che evidenzia come il gatekeeper dovrebbe astenersi da qualsiasi forma di trattamento differenziato o preferenziale ai fini del posizionamento sul servizio di piattaforma di base, e relativa indicizzazione crawling, attraverso strumenti giuridici, commerciali o tecnici, che favorisca prodotti o servizi offerti dal gatekeeper stesso o attraverso un utente commerciale sottoposto al suo controllo. Per garantire che tale obbligo risulti efficace, anche le condizioni applicate a tale posi-

mento differenziato o preferenziale[39] vietata ai sensi dell'articolo 5 mediante l'imposizione di obblighi specifici diretti ad evitare uno sfruttamento dei dati degli utenti finali, anche mediante combinazione, e provenienti da più servizi. Inoltre, il successivo articolo 6 (comma 5) precisa che "il gatekeeper non garantisce un trattamento più favorevole, in termini di posizionamento e relativa indicizzazione e crawling, ai servizi e prodotti offerti dal gatekeeper stesso rispetto a servizi o prodotti analoghi di terzi ed applica condizioni trasparenti, eque e non discriminatorie a tale posizionamento"[40]. Infine, i commi 9, 10, 11 e 12 disciplinano i termini di accesso agli strumenti di misurazione delle prestazioni nonché la portabilità dei dati dell'utente finale.

Proprio la lettura combinata dei due articoli appare importante perché, quanto stabilito all'art. 6 avrebbe potuto lasciare spazi di interpretazione al gatekeeper per addurre, ad esempio, che il posizionamento mostrato non deriva da un intento di favorire i propri prodotti, frutto di uno sfruttamento dei dati degli utenti finali, bensì, ad esempio, da una semplice aggregazione numerica delle scelte da essi effettuate.

---

zionamento dovrebbero essere generalmente eque e trasparenti. In tale contesto il posizionamento dovrebbe contemplare tutte le forme di rilevanza relativa, compresi visualizzazione, valutazione, collegamenti o risultati vocali e dovrebbe comprendere anche i casi in cui un servizio di piattaforma di base presenta o comunica un solo risultato all'utente finale. Per garantire l'efficacia e l'ineludibilità di questo obbligo è opportuno applicarlo del pari a qualsiasi misura che abbia un effetto equivalente al trattamento differenziato o preferenziale ai fini del posizionamento.

[39] Nel caso Google Search Shopping, Decisione C (2017) 4444, n. AT39740, (*https://competition-cases.ec.europa.eu/cases/AT.39740*), era stata ravvisata una condotta di autopreferenza ed anche in questo caso non si utilizzava questa qualificazione bensì, come poi inserito nel DMA, quella di trattamento più favorevole connesso a condotte escludenti e rifiuti impliciti di fornitura come si evince anche dalla sentenza della Corte di Giustizia relativa alla decisione, causa T-612/17 e C-48/22 P, del 10 settembre 2024.

[40] Previsioni analoghe dal punto di vista dei comportamenti che danno luogo ad autopreferenza si riscontrano anche nel UK Digital Markets, Competition and Consumer Act, del maggio 2024, all'art. 20 co. 3 lett. a-h. Più in generale si veda il position paper della Competition Market Authority (CMA) e dell'Information Commisioner's Office (ICO), Harmful design in digital markets: How Online Choice Architecture practices can undermine consumer choice and control over personal information, 2023, *https://www.drcf.org.uk/siteassets/drcf/pdf-files/harmful-design-in-digital-markets-ico-cma-joint-position-paper.pdf?v=380506*.

La scelta di procedere con l'introduzione di specifici obblighi il cui rispetto verrà monitorato dalla Commissione appare una scelta che, in combinazione con i procedimenti per violazione delle condotte ed applicazione delle relative sanzioni economiche può produrre effetti e andare nella direzione di ridurre la posizione di forza che questi soggetti rivestono attualmente nel mercato alimentata dall'autopreferenza (e non solo). Una valutazione sull'efficacia del provvedimento non può però non tenere conto dell'influenza esercitata anche dai comportamenti degli utenti nonché di un possibile mutamento di quelli delle c.d. Big Tech che potrebbero porre in essere nuove ed ulteriori modalità di restrizione della concorrenza all'interno dei loro ecosistemi e non solo. Questa seconda eventualità, del resto, emerge dalla stessa formulazione del DMA laddove si prevede il monitoraggio di quanto previsto e la possibilità di eventuali successive modifiche. In tal senso, come sarà evidenziato nelle riflessioni conclusive, è utile ricordare come, proprio nel mese di settembre del 2025, si sia chiusa una consultazione pubblica diretta a svolgere un'analisi anche sull'efficacia del DMA rispetto agli obiettivi di contendibilità ed equità[41].

## 3. *Le acquisizioni quale "strumento" di creazione e consolidamento di un ecosistema e l'applicabilità della normativa europea sulle concentrazioni*

Nell'esame dei fattori capaci di alterare la contendibilità dei mercati sono da annoverare anche le concentrazioni in quanto "strumento", come emerge dai dati sulle operazioni concluse, utilizzato dagli ecosistemi sia per l'ampliamento della propria offerta in segmenti di mercato differenziati, sia per il consolidamento al fine di incrementare la loro innovatività e capacità espansiva in sempre nuovi e differenti segmenti di mercato[42]. Anche per questo

[41] La consultazione promossa dalla DG Competition e da quella Communications Networks, Content and Technology era stata aperta il 3 luglio 2025 e si è conclusa il 24 settembre. Si veda *https://digital-markets-act.ec.europa.eu/consultation-first-review-digital-markets-act_en#why-we-are-consulting*.

[42] Dalla sua fondazione Google ha fatto più di 200 acquisizioni. Solo per citarne alcune avvenute tra il 2006 ed il 2014 che hanno differenziato e consentito lo sviluppo

il ricorso alle acquisizioni è stato utilizzato con una certa sistematicità ed ha riguardato non solo imprese medio-grandi, ma anche piccole proprio per la loro capacità di garantire possibili innovazioni.

Infatti, l'acquisizione di start-up "promettenti" può dare luogo ad un duplice vantaggio per il gatekeeper non solo in termini di innovazione, ma anche di eliminazione dal mercato di un potenziale futuro concorrente, seppur su un segmento specifico, ed anche per questo sono state spesso qualificate come acquisizioni *killer*[43]. Inoltre, va segnalato come le acquisizioni effettuate dalle piattaforme abbiano un'ulteriore implicazione rispetto a quelle "tradizionali" in quanto consentono anche un arricchimento del patrimonio informativo attraverso l'integrazione di quello del soggetto acquisito,

---

di Google, oltre ad essere fra le più dispendiose dal punto di vista economico si possono ricordare quella di: YouTube nel 2006; DoubleClick provider di software per la gestione dell'advertising online avvenuta nel 2007; Postini Communication Security nel 2007; AdMobe mobile advertising nel 2009; ITA Software, Travel Technology nel 2010; Motorola Mobility operante nell'ambito dei media nel 2011; Admeld Online Advertising nel 2011; Wildfire Interactive, Social Media Marketing; Waze software di navigazione GPS nel 2013; Nest operante nel settore della domotica ed in particolare di dispositivi domestici connessi ad internet nel 2014. L'*Economist*, il 26 ottobre del 2018, in un articolo American tech giants are making life tough for startups, sottolineava come Google nel periodo 2011-2018 avesse acquistato un'impresa al mese e come non fosse l'unico soggetto particolarmente attivo nelle acquisizioni, visto che nel 2017 Alphabet, Apple, Amazon, Facebook e Microsoft avessero speso 31,6 miliardi di acquisizioni di start-up.

[43] Tali acquisizioni sono state anche definite "killer" perché capaci di conferire il duplice obiettivo di eliminare un potenziale concorrente sul mercato acquisendo contestualmente il suo know how. Sull'utilizzo del termine "killer" in queste situazioni si vedano in particolare C. Cunningham, F. Ederer, S. Ma, *Killer acquisitions*, 2019, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3241707*; M. Bourreau, A. De Streel, *Digital conglomerates and EU competition policy*, Centre on Regulation in Europe (CERRE), 2019, *https://cerre.eu/news/digital-conglomerates-and-eu-competition-policy/*; K.C. Limarzi, H.R.S. Phillips, *"Killer Acquisitions", Big Tech and section solution in search of a problem*, 26 May 2020, *Antitrust Chronicle*, *www.competitionpolicyinternational.com*; A. Canepa, *I mercanti dell'era digitale, Contributo allo studio delle piattaforme*, Giappichelli, Torino, 2020, p. 103 ss.; OECD, *Start-ups, Killer Acquisitions and Merger Control*' Background Note, May 2020, DAF/COMP(2020)5, *https://www.oec.d.org/en/publications/start-ups-killer-acquisitions-and-merger-control_dac52a99-en.html*; K.A. Bryan, E Hovenkamp, *Antitrust Limits on Startup Acquisitions*, *Review of Industrial Organization*, 2020, p. 615 ss.; M. Ivaldi, N. Petit, S. Unekbas, *Killer Acquisitions: Evidence from European Merger Case*s, Working paper n. 1420/2014, Toulouse School of Economics, 2023, *https://www.tse-fr.eu/sites/default/files/TSE/documents/doc/wp/2023/wp_tse_1420.pdf*.

come mostrano sia il caso dell'acquisizione di Whatsapp da parte di Facebook che il caso di Shazam, sviluppatore di applicazioni di riconoscimento musicale, da parte di Apple[44].

La normativa europea in materia, ed in particolare il Reg. 139/2004, al fine di evitare un eccessivo rafforzamento su un determinato mercato anche grazie all'eliminazione di concorrenti, stabiliva già dal 2004 un controllo a seguito di notifica, da effettuare preventivamente all'operazione, in tutti i casi nei quali l'impresa da acquisire aveva un fatturato totale superiore ad una certa soglia. La finalità di tale verifica era quella di individuare le situazioni capaci di determinare un ostacolo ad una concorrenza effettiva. Inoltre, si precisava come dovesse essere considerata una concentrazione comunitaria soggetta a tali previsioni anche la situazione nella quale le imprese non avessero sede o riferimento principale della loro attività nella Comunità europea ma vi svolgessero attività sostanziali[45]. Fatta salva la possibilità di intervento a livello nazionale, le concentrazioni "sotto-soglia" tra le quali possono figurare proprio quelle relative a start-up risultavano escluse dal controllo stabilito dal Regolamento. Alla luce però del loro possibile rilievo nel mercato digitale sul punto la Commissione aveva aperto una riflessione e, nel 2021, in un documento di analisi, degli aspetti procedurali e giurisdizionali era stato evidenziato come, sebbene le soglie previste fossero state generalmente efficaci nel rilevare operazioni con un significativo impatto negativo sulla concorrenza nel mercato interno, ve ne fossero alcune, potenzialmente pregiudizievoli, sfuggite al rie-

[44] Si tratta rispettivamente di Commissione Europea, caso M8228, Facebook/Whatsapp, 17 maggio 2017 e caso M.8788, Apple/Shazam. In quest'ultimo caso secondo la Commissione però l'acquisizione dei dati degli utenti non rappresenterebbe un ostacolo significativo alla concorrenza visto che "altri operatori di streaming di musica digitale raccolgono informazioni e dispongono di banche dati su appassionati di musica simili a Apple Music e potrebbero potenzialmente associarsi a fornitori di servizi di pubblicità, se questo tipo di dati dovesse risultare necessario per competere nel segmento degli appassionati di musica". Si veda il punto 32 della decisione del 6 settembre 2018 in GUUE C 417/4 del 16 novembre 2018.

[45] Si veda il considerando 10 del Regolamento 139/2004. L'art. 1 indicava le soglie quantitative previste di fatturato. È utile ricordare come nel 2023 siano state adottate due Comunicazione della Commissione C(2023)2401 final e C (2023)2402 del 20 aprile 2023 nonché un Regolamento per l'esecuzione del Reg. 139/2004 tutti volti a semplificare e rendere più efficace la procedura di controllo.

same da parte sia della Commissione che degli Stati membri[46]. Per tali motivi era stata adottata una comunicazione, contenente orientamenti per alcune tipologie di casi[47], diretta ad individuare alcune situazioni potenzialmente valutabili attraverso il meccanismo del rinvio in quanto l'operazione non era soggetta a notifica. Proprio secondo questo schema, era stato sottoposto a valutazione un progetto di acquisizione nel settore farmaceutico della società Grail da parte di Illumina. Nel caso di specie non risultavano raggiunte le soglie di fatturato richieste dal Regolamento, ma la Commissione aveva accolto una richiesta in tal senso dall'autorità nazionale francese in materia di concorrenza. Infatti, la Commissione aveva ritenuto che l'operazione, proprio per le sue caratteristiche, avesse il potenziale per incidere sugli scambi in quanto la rilevanza concorrenziale di Grail era maggiore di quanto si potesse evincere dal semplice esame del suo fatturato. Per tali motivi era intervenuta sanzionando la realizzazione della concentrazione prima dell'approvazione[48] . La Corte di Giustizia, però, proprio esaminando il caso in oggetto, aveva annullato la decisione di accoglimento da parte della Commissione della richiesta francese, ritenendo che l'articolo 22 del regolamento sulle concentrazioni non autorizzasse l'accettazione di rinvii di concentrazioni da parte di Stati membri che non sono competenti ad esaminare tali concentrazioni ai sensi del loro diritto nazionale[49].

---

[46] Si veda il documento di lavoro dei servizi della Commissione sulla valutazione degli aspetti procedurali e giurisdizionali del controllo delle concentrazioni nell'UE (SWD(2021) 66 final del 26 marzo 2021.

[47] Comunicazione della Commissione - Orientamenti della Commissione sull'applicazione del meccanismo di rinvio di cui all'articolo 22 del regolamento sulle concentrazioni per determinate categorie di casi, C (2021) 1959, GU C 113 del 31.3.2021.

[48] Sulla questione vi sono state anche una serie di decisioni adottate dalla Commissione, e nello specifico: la decisione del 22 luglio 2021, relativa all'avvio di una fase II di indagine sul progetto di acquisizione di GRAIL da parte di Illumina (caso COMP/M.10188); la decisione adottata il 6 settembre 2022 di divieto dell'acquisizione di GRAIL da parte di Illumina (caso M.10188); due decisioni relative a provvedimenti provvisori rispettivamente del 29 ottobre 2021 (M.10493) e del 28 ottobre 2022 (caso M.10938); iv) la decisione del 12 ottobre 2023 relativa a misure di ripristino che imponevano alla Illumina di annullare l'acquisizione di GRAIL (caso M.10939) ed infine la decisione adottata il 12 luglio 2023 che sanzionava Illumina e GRAIL per aver realizzato la concentrazione prima dell'approvazione della Commissione (caso M.10483). Tali decisioni sono state revocate.

[49] Proprio quanto stabilito dalla Corte di Giustizia aveva portato la Commis-

Allo stesso tempo, un'altra sentenza della Corte di Giustizia[50], aveva evidenziato un aspetto molto importante per le c.d. "acquisizioni seriali" e cioè quelle che, pur essendo poste in essere in momenti differenti, potrebbero sembrare prive di un collegamento tra di loro, ma sono in realtà parte di un disegno complessivo e vengono spesso utilizzate dagli ecosistemi. In tali casi, secondo la Corte, le singole operazioni di fusione possono essere oggetto di una valutazione congiunta qualora risultino strettamente collegate tra loro con un vincolo condizionale o siano strutturate come una serie di transazioni concluse in un breve lasso di tempo.

Sulle concentrazioni, oltre agli interventi volti a modificare e velocizzare le procedure di controllo nonché quelli attuati a livello nazionale[51], è poi intervenuto anche il DMA che ha stabilito a ca-

---

sione ad adottare una nuova comunicazione, la C2024/7190 del 2 dicembre 2024 relativa al ritiro dell'atto 2021/C113/01. Per un commento alla sentenza si vedano in particolare B.L. ALDERMAN & R.D. BLAIR, *Reflection on the Illumina Grail merger*, *Journal of Antitrust Enforcement*, vol. 11, Issue 3, novembre 2023, p. 536 ss.; J. MULDER, W. SAUTER, *A new regime for below threshold mergers in EU competition law? The Illumina/Grail and Towercast judgments*, Journal of Antitrust Enforcement, vol. 11, Issue 3, novembre 2023, p. 544; P. WHEELAN, *EU-level jurisdiction over "Killer Acquisitions" in the aftermath of Illumina/Grail*, in *Antitrust Chronicle*, December 2024; W. SAUTER, J. MULDER, *Merger jurisdiction in EU competition law after Illumina/Grail: What's next?*, in *Journal of Antitrust Enforcement*, marzo 2025, p. 215 ss. e J. LINDEBOOM, *Illumina/Grail: flawed originalism and the judicial hunch*, in Idem, p. 223 ss.

[50] Si veda la sentenza CGCE, caso C-449/21, Towercast SASU v. Autoritè de la cuncurrence, Ministre chargè de l'economie, del 16 marzo 2023, *www.curia.eu*.

[51] È utile ricordare come in Italia la Legge per il mercato e la concorrenza 2021, L. 118/2022, abbia introdotto il co. 1-*bis* all'art. 16 della L. 287/90 che stabilisce come "l'Autorità può richiedere alle imprese interessate di notificare entro trenta giorni un'operazione di concentrazione anche nel caso in cui sia superata una sola delle due soglie di fatturato di cui al comma 1, ovvero nel caso in cui il fatturato totale realizzato a livello mondiale dall'insieme delle imprese interessate sia superiore a 5 miliardi di euro, qualora sussistano concreti rischi per la concorrenza nel mercato nazionale, o in una sua parte rilevante, tenuto anche conto degli effetti pregiudizievoli per lo sviluppo e la diffusione di imprese di piccole dimensioni caratterizzate da strategie innovative, e non siano trascorsi oltre sei mesi dal perfezionamento dell'operazione". Sull'esercizio di questi poteri anche in rapporto alla sentenza Illumina Grail si veda in particolare E. FRENI, *Le concentrazioni sotto soglia tra realtà e falsi miti: alcuni spunti dalla prassi applicativa*, in *Riv. Reg. Merc.*, 2025, p. 68 ss. Più in generale sul nuovo assetto della disciplina italiana in materia compresa la possibilità di valutazione a livello nazionale anche di imprese di piccole dimensioni caratterizzate da strategie innovative si veda F. GHEZZI, M.T. MAGGIOLINO, *La nuova disciplina di controllo delle concentrazioni in Italia: alla ricerca di una convergenza con il diritto europeo*, in *Riv. Soc.*,1, 2023, p. 32 ss.

rico dei gatekeeper un obbligo di informazione della Commissione su qualunque progetto di concentrazione, a prescindere dal raggiungimento della soglia, qualora le entità partecipanti alla concentrazione o l'oggetto della concentrazione forniscano servizi di piattaforma di base o qualsiasi altro servizio nel settore digitale o consentano la raccolta di dati[52].

Il principale problema però nella valutazione delle concentrazioni, in particolare quelle di interesse degli ecosistemi, è da individuare non solo e non tanto in elementi procedurali quanto nella complessità di valutazione delle singole acquisizioni, in particolare in ambito digitale, per le quali, come del resto dimostra proprio il caso delle start-up, non è sufficiente valutare solo il prezzo e l'attuale ambito di operatività ma si dovrebbe tenere conto anche delle implicazioni che l'acquisizione di un soggetto innovativo può generare nello sviluppo futuro dell'acquirente[53].

## 4. *Dal regolamento n. 1/2003 al DMA: una nuova evoluzione nei rapporti tra Commissione e autorità nazionali?*

Nel quadro di una valutazione complessiva della normativa vigente appare di interesse affiancare all'esame delle singole condotte anche qualche considerazione sull'assetto organizzativo e la ripartizione di competenze tra autorità nazionali ed europee.

Tali riflessioni appaiono di interesse in particolare alla luce del ruolo attribuito alla Commissione ed alle autorità nazionali dal Regolamento n. 1/2003, consolidato anche con la direttiva n. 1/2019[54]. Come noto, il regolamento n. 1/2003 aveva delineato un nuovo assetto di tipo decentrato con un ruolo maggiore delle autorità nazionali proprio per dare luogo ad un incremento di efficacia ed efficienza. Nello specifico veniva superato il sistema centralizzato disegnato dal precedente regolamento, il n. 17/1962, che individuava la

---

[52] Si veda il Regolamento 1925/2022 art. 14 co. 1.

[53] Questo aspetto è evidenziato anche dal Rapporto Draghi, *The future of European competitiveness*, Parte B, settembre 2024, Cap. 4 p. 299.

[54] Si tratta del Regolamento n. 1/2003 del Consiglio, del 16 dicembre 2002, concernente l'applicazione delle regole di concorrenza di cui agli articoli 81 e 82 del trattato in GU L1 del 4 gennaio 2003.

Commissione come il soggetto competente a "constata(re) su domanda o d'ufficio, un'infrazione alle disposizioni dell'articolo 85 o dell'articolo 86 del Trattato" e poteva "obbliga(re), mediante decisione, le imprese ed associazioni di imprese interessate a porre fine all'infrazione constatata"[55]. Il considerando 4 del Regolamento n. 1/2003 sottolineava come tale sistema sarebbe stato "sostituito con un sistema di eccezione direttamente applicabile, in base al quale le autorità garanti della concorrenza e le giurisdizioni degli Stati membri siano competenti non solo ad applicare l'articolo 81, paragrafo 1 e l'articolo 82 del trattato, ma anche l'articolo 81, paragrafo 3".

Proprio alla luce di quanto brevemente richiamato, si comprende perché sia utile soffermarsi sull'assetto complessivo derivante anche dall'approvazione del DMA che, a partire dalle modalità di individuazione dei gatekeepers, per poi arrivare al controllo sul rispetto degli obblighi introdotti dal DMA, mostra un'apparente discontinuità rispetto alla ripartizione delle competenze appena delineata.

Infatti, ai sensi dell'articolo 3 e dei successivi, la designazione di un gatekeeper, l'eventuale revisione ed il rispetto degli obblighi conseguenti vengono effettuati dalla Commissione anche se poi l'art. 38 individua modalità di coordinamento e cooperazione tra la Commissione e le autorità nazionali alle quali è consentito l'avvio di un'indagine sui gatekeeper sulla base della legislazione nazionale, previa comunicazione alla Commissione. Non vi sono però ulteriori indicazioni, ad eccezione del piano operativo di scambio delle informazioni, su come verrà gestito il procedimento nei differenti scenari che in concreto potrebbero aprirsi[56] fatta salva la collaborazione investigativa e lo scambio delle informazioni in linea con quanto stabilito dal Reg. n. 1/2003 sull'European Competition Network.

---

[55] Si veda il Regolamento n. 17 del 1962 Primo regolamento d'applicazione degli articoli 85 e 86 del Trattato e pubblicato nella GU 13 del 21.2.1962, pp. 204, articolo 3 co. 1 e 2.

[56] Per un esame proprio delle differenti possibilità di interazione tra i due livelli di governo si veda in particolare A. Ribera Martinez, *The decentralisation of the DMA enforcement System*, *GRUR International*, *Journal of International IP Law*, Vol. 73, Issue 12, dicembre 2024, p. 1111 ss.

In sostanza, si potrebbe affermare che il DMA riconosca un ruolo guida alla Commissione[57] quale soggetto deputato all'applicazione delle misure introdotte, mentre soltanto compiti di monitoraggio e cooperazione alle autorità nazionali nel momento in cui applicano la normativa nazionale nei confronti dei gatekeepers.

Sulla questione già nel 2021 la Commissaria Vestagher aveva evidenziato come non vi sarebbe stata un'influenza sul modo in cui le regole di concorrenza già esistenti trovavano applicazione nei mercati digitali ed aveva aggiunto come non sarebbero mutati neppure i poteri della Commissione o delle autorità nazionali garanti della concorrenza volte a far rispettare tali regole nel mondo digitale[58].

Inoltre, il considerando 11 del DMA, con riferimento agli articoli 101 e 102 del TFUE, sottolineava una differenziazione tra le due normative sulla base degli obiettivi perseguiti che sembrava voler indicare anche la necessità di una differenziazione sul piano applicativo. Infatti, si sottolineava come queste disposizioni e "le corrispondenti norme nazionali in materia di concorrenza relative a comportamenti anticoncorrenziali unilaterali e multilaterali, come pure al controllo delle concentrazioni, si prefiggono quale obiettivo la protezione della concorrenza non falsata sul mercato. Il presente regolamento persegue un obiettivo complementare, ma diverso (…) e tale obiettivo consiste nel garantire che i mercati in cui sono presenti gatekeeper siano e rimangano equi e contendibili".

La ratio di un'impostazione centralizzata come quella introdotta dal DMA sembrava pertanto dettata da esigenze di riduzione delle differenziazioni e frammentazioni derivanti dall'azione a livello nazionale e circoscritta alle azioni di tutela della contendibilità ed equità. Del resto, la presenza di possibili criticità sotto questo profilo, anche dal punto di vista legislativo, era emersa già in sede di discussione del DMA. In tal senso basti pensare, all'intervento

---

[57] L'articolo 1 (7) aggiunge: "Le autorità nazionali non adottano decisioni in contrasto con una decisione adottata dalla Commissione ai sensi del presente regolamento".

[58] Si veda l'intervento di Margrethe Vestager, Competition in the Digital Age, European Internet Forum, 17 marzo 2021, *https://ec.europa.eu/newsroom/comp/items/705929*.

adottato in Germania che attribuiva all'autorità garante nazionale il potere di individuare le imprese con un ruolo rilevante sul mercato tale da pregiudicare la concorrenza[59].

Alla luce di quanto enucleato, si potrebbe ritenere che vi sia solo una variazione di assetto circoscritta alle peculiarità delle grandi piattaforme e ad essa limitata. In realtà, una simile impostazione mette in luce due rischi tra loro differenti e definibili: uno di tipo più operativo ed uno di ripartizione chiara di competenze. Il primo riguarda un possibile scarso incentivo delle autorità nazionali alla luce del ruolo loro riconosciuto di mero supporto al lavoro della Commissione. Il secondo, invece, concerne la gestione del rapporto tra le leggi nazionali che implicano una logica di contendibilità ed equità ed il DMA. Infatti, sia per la contendibilità che per l'equità, l'individuazione di un perimetro di azione basato su questi due termini risulta tutt'altro che netta, vista anche la difficoltà di una chiara distinzione delle fattispecie incluse. Sulla complessità del concetto di contendibilità ci si è già soffermati, ma anche l'equità pone questioni simili[60]. Ai sensi di alcuni considerando e articoli del DMA[61], questa sembrerebbe da riferire in modo particolare allo squilibrio tra utenti commerciali e gatekeeper sia esterno all'ecosistema che interno, come nel caso del marketplace di Amazon e in presenza di condotte come l'autopreferenza. Del resto, la definizione degli obblighi previsti a carico dei gatekeepers appare incentrata sullo sfruttamento della posizione dominante ed sulla capacità di esclusione strettamente connesse all'applicazione dell'art. 101.

---

[59] Si veda l'art. 1 del Competition Act, come modificato dall'Atto del 25 ottobre 2023, Federal Law Gazette I, p. 294. *https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html*. Per un approfondimento OECD, Directorate for Financial and Enterprise Affairs Competition Committee, Annual Report on Competition Policy Developments in Germany 2023, 18 giugno 2024, DAF/COMP/AR(2024)13, *https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Taetigkeitsberichte/OECD-AnnualReport2023.pdf?__blob=publicationFile&v=3*.

[60] Sul punto si veda in particolare D. Zimmer, N. Nittenwilm, *For Whose Sake, and by Which Means? Fairness Concepts in European Law. A Reflection on the Occasion of Recent European Legislation, Especially the Passage of the Digital Markets Act*, Zeitschrift für europäisches Privatrecht, 2022, p. 820 ss.

[61] Si vedano in particolare l'art. 12 co. 5 ed il considerando 33 del DMA.

In tale quadro, proprio l'esame dei rimedi introdotti, rende difficile ritenere che tale concetto non includa anche il rapporto con l'utente finale e la sua tutela attraverso non solo una garanzia di un mercato più competitivo ma anche di una minore capacità di indirizzo e condizionamento delle scelte attraverso lo sfruttamento dei dati, il posizionamento delle offerte, le difficoltà di valutazione di tutte le alternative. Infatti, seppur in via indiretta, si può ritenere che il legislatore abbia disegnato le previsioni tenendo conto non solo delle implicazioni sugli utenti commerciali, ma anche su quelli finali. Ciò renderebbe la definizione molto più ampia anche dal punto di vista dei potenziali comportamenti inclusi con tutto ciò che ne consegue in termini di ampliamento delle situazioni caratterizzate dall'applicazione di uno schema centralizzato. Infine anche i procedimenti ai sensi del DMA e quelli relativi alle condotte anticoncorrenziali, in particolare ai sensi dell'art. 101 TFUE, in assenza di una netta distinzione, pur essendo pensati su binari paralleli e complementari, rischierebbero di avere intrecci anche ai sensi del principio del *ne bis in idem*[62].

## 5. *Qualche considerazione conclusiva*

Come evidenziato anche dal Rapporto Draghi, il livello delle concentrazioni industriali registra un incremento, così come aumentano sempre di più la differenziazione di performance e gli squilibri tra alcuni grandi operatori, soprattutto nei mercati digitali, e gli altri[63]. Una simile evoluzione rileva non solo sul piano dimensionale, ma anche perché i grandi operatori sono diventati tali anche grazie ad un nuovo modello di business incentrato sulla tecnologia e sulla capacità di sfruttarla. La posizione di forza sul mercato che questi operatori hanno acquisito non ha modificato solo gli equilibri concorrenziali, ma anche i parametri di riferimento, visto che l'innovatività supera per importanza le politiche di prezzo e

[62] Sul punto in particolare N. Moreno Belloso, N. Petit, *The Eu Digital Markets Act. A Competition Hand in a Regulatory Glove*, in Eur. Law. Rev., 2023, p. 418 ss.

[63] Si veda il Rapporto Draghi, *The future of European competitiveness…*, cit., p. 298.

l'essere concorrenziali risulta secondario rispetto alla possibilità di diventare "controllori" del mercato ed avere la capacità di mantenere nel tempo questo ruolo.

Tutto ciò inevitabilmente ha imposto anche un ripensamento degli strumenti a disposizione per tutelare la concorrenza e per intervenire su tutti gli aspetti che hanno contribuito e contribuiscono a consolidare un simile assetto. La valutazione su nuovi interventi e modifiche dell'esistente è però resa più complessa dalla rapidità dello sviluppo tecnologico che può anche minarne l'efficacia.

In un simile quadro, come evidenziato, rilevano più aspetti dallo sfruttamento dei dati per rafforzare il proprio vantaggio sul mercato fino alla possibilità di concludere molteplici acquisizioni, espandersi in altri segmenti di mercato e perfino garantirsi nuove idee o applicazioni tecnologiche come nel caso delle start up. Ciò significa che se ci soffermiamo sulla normativa europea dobbiamo esaminare l'efficacia della previsione di condotte anticoncorrenziali sanzionabili come quelle di abuso di posizione dominante, compresa la sua declinazione di abuso di dipendenza economica, nonché le previsioni del DMA e quelle sulle concentrazioni. Di queste ultime, alla luce dell'attuale assetto della disciplina, rileva in particolare la necessità di valutazioni più articolate nei mercati digitali che tengano conto non solo dell'impatto attuale di mercato, comprensivo delle dinamiche di prezzo, che le singole operazioni potrebbero generare, ma anche dei possibili sviluppi futuri e delle relative implicazioni. Ciò, come evidenziato, può significare una valutazione anche di casi che non raggiungano la soglia prevista di controllo perché la componente di innovazione delle start up ha una dimensione strategica che va oltre il loro fatturato al momento dell'acquisizione ed anche un esame attento delle acquisizioni in serie utili per l'espansione dell'ecosistema.

Segnali in tal senso sono ravvisabili sia in alcune scelte delle normative nazionali, compresa quella italiana alla luce delle ultime modifiche alla L. 287/90, nonché negli interventi giurisprudenziali, in particolare, della Corte di Giustizia[64]. Permangono però ancora

[64] È utile ricordare come non manchino indicazioni sulla necessità di una valutazione attenta ai fini dell'individuazione di un'impossibilità di procedere. In tal senso,

elementi di criticità in grado di incidere anche sull'efficienza dovuti alla complessità procedurale, nonostante gli interventi del 2023[65], ed alla necessità di monitoraggio in contemporanea di tutti i segmenti di mercato che può incidere anche sui tempi di intervento.

Se consideriamo i nuovi interventi come il DMA e l'importanza di poter disporre anche di un intervento *ex ante* oltre che *ex post* va rilevato come questo abbia già consentito, alla luce degli obblighi introdotti, l'avvio di procedimenti, ad esempio nei confronti di Apple e Meta[66], e la relativa applicazione di sanzioni anche con una certa rapidità. Infatti, l'attuale Presidente degli Stati Uniti, nell'ambito della trattativa tra Stati Uniti ed Ue sull'introduzione di dazi, le ha definite, dannose e discriminatorie per alcune imprese come le Big Tech statunitensi[67]. Ciononostante, proprio la fase applicativa, renderà più chiaro se l'assetto organizzativo delineato possa essere considerato efficiente e privo di sovrapposizioni di competenze alla luce del decentramento previsto dal Reg. n. 1/2003 e se potrà rimanere efficace nel tempo. Quest'ultimo, in particolare, è uno degli aspetti più difficili da valutare in quanto alcune delle

ad esempio, il Tribunale nel caso T-399/16, CK Telecoms c. Commissione del 28 maggio 2020 ricorda come la concorrenza tra i due soggetti oggetto della fusione e la conseguente riduzione complessiva della concorrenza non siano elementi di per sé sufficienti per bloccare l'acquisizione.

[65] Il riferimento è in particolare alla Comunicazione 2023/C160/02 recante esecuzione del regolamento (CE) n. 139/2004 del Consiglio relativo al controllo delle concentrazioni tra imprese e che abroga il regolamento (CE) n. 802/2004 della Commissione che ha specificato il formato da utilizzare per le notifiche, le richieste motivate, le osservazioni relative alle obiezioni della Commissione, gli impegni proposti dalle imprese interessate nonché il Regolamento di esecuzione n. 914/2023.

[66] Si tratta del caso DMA100020 Meta online social networking services, DMA.100024 Meta - number-independent interpersonal communications services DMA.100035 Meta - online advertising services DMA.100044 Meta - online intermediation services - market concluso con decisione della Commissione C(2023)6105 del 5 settembre 2023 e del caso DMA 100055 Meta concluso con decisione della Commissione C(2025)2091 del 23 aprile 2025.

[67] Si vedano in tal senso i numerosi articoli di stampa pubblicati a seguito di alcune dichiarazioni del Presidente Trump. Tra di essi *https://www.eunews.it/2025/08/26/trump-minaccia-chi-regola-le-attivita-delle-aziende-digitali-lue-risponde-da-noi-le-regole-le-facciamo-noi/*, *https://www.editorialedomani.it/politica/europa/dazi-big-tech-digitale-ue-trump-von-der-leyen-c8aobpz9*; *https://www.corriere.it/economia/opinioni/25_ottobre_01/la-diga-digitale-va-difesa-contro-il-far-west-di-trump-f6fc038a-6ee3-4fea-962c-f56621809xlk.shtml*.

previsioni introdotte sono una fotografia della situazione osservata in questi anni e analizzate nei procedimenti condotti per violazione della concorrenza ai sensi delle previsioni del TFUE. Proprio però la rapidità dello sviluppo tecnologico ed in particolare dell'intelligenza artificiale, fulcro del modello di business di queste piattaforme per la personalizzazione ed offerta di nuovi servizi, potrebbe modificare in parte il quadro attuale ed anche le condotte oggi individuate. Del resto, che questo scenario sia già in parte una realtà lo dimostra proprio l'apertura nel settembre di quest'anno di una prima consultazione, avviata dalla DG Competition, focalizzata sugli sviluppi dell'intelligenza artificiale e sulle implicazioni nell'azione delle piattaforme che controllano i mercati alla luce della gestione dei modelli di intelligenza artificiale generativa e dei prodotti che la incorporano nonché della relativa interoperabilità capace di conferire un indubbio vantaggio a chi ne può disporre.

C'è infine un ultimo elemento da tenere in considerazione nella valutazione sul grado di efficacia delle previsioni introdotte ed è quello del comportamento degli utenti e dei loro bias cognitivi capaci di avere rilievo da due punti di vista. Infatti, i bias possono rilevare in rapporto ad alcuni degli obblighi previsti ed alla loro capacità di risultare efficaci proprio alla luce delle scelte adottate dagli utenti. Basti pensare solo per fare un esempio, al riconoscimento dell'interoperabilità non così semplice da sfruttare per tutti gli utenti e tale da poter scoraggiare una parte, con inevitabili conseguenze sui risultati auspicati in termini di modifiche preferenziali degli utenti. Peraltro, anche in presenza di previsioni volte a stimolare una comparazione e l'esercizio di una scelta tra più opzioni, ben mostrato in altri segmenti di mercato, come i servizi pubblici, numerosi sono i fattori che possono influenzare le decisioni degli utenti, compreso il mantenimento dello *status quo* anche quando, ad esempio, le condizioni economiche potrebbero suggerire l'opportunità di un cambiamento[68].

Tali aspetti si riscontrano anche nei mercati digitali dove la personalizzazione dell'offerta ed i processi di fidelizzazione, anche

[68] Per una ricognizione ad ampio spettro sui bias comportamentali si veda in particolare F. VELLA, *Diritto ed economia comportamentale*, Il Mulino, Bologna, 2023.

semplicemente per le ricerche, oltreché per gli acquisti di beni o servizi, sono ormai apprezzate dagli utenti ed hanno modificato profondamente i processi decisionali di acquisto e selezione dei servizi risultando non semplici da modificare. Importanti, nel percorso di "rieducazione" ad una piena capacità di comparazione e scelta appaiono le previsioni, definite "antielusione" dell'art. 13 del DMA laddove si si fa riferimento esplicitamente alla necessità che la piattaforma non debba alterare le condizioni o le qualità dei servizi nè rendere l'avvalersi di diritti o scelte oltremodo difficile "attraverso la struttura, la progettazione, la funzione o le modalità di funzionamento di un'interfaccia utente o di una parte della stessa"[69]. La ratio è quella di intervenire su una molteplicità di aspetti dall'opzione predefinita fino alle modalità con le quali vengono ordinate e presentate le offerte (effetti di ranking) e la loro identificazione. Si tratta di condotte che possono essere realizzate in vario modo e verificarsi anche quando, ad esempio, vi sia stata la scelta di modifica dell'operatore e del servizio utilizzato al fine di favorire un "ritorno indietro"[70]. Peraltro, il DMA proprio all'opzione predefinita dedica una previsione specifica (art. 6 co. 3) attraverso la quale interviene in modo diretto stabilendo, in sede di primo utilizzo, quella che potremmo definire una "scelta attiva" dell'utente finale tra una serie di opzioni proposte. Inoltre, ha correttamente incluso nelle previsioni di tutela anche gli utenti commerciali e non solo quelli finali perché, come descritto nel caso di Amazon, proprio coloro che vendono attraverso il marketplace sono condizionati nelle loro decisioni di permanenza e definizione delle condizioni di vendita senza neppur poter prendere in considerazione alternative. Simili previsioni possono contribuire non solo direttamente ma anche indirettamente nel favorire un incremento di attenzione degli utenti finali sulle proprie scelte con possibili effetti favorevoli di sistema.

---

[69] Si tratta dell'art. 13 co. 6 del DMA.

[70] Sulla necessità di valutazioni delle single situazioni si veda la ricerca commissionata dall'European Consumer Organisation (BEUC), *Examining the Design of Choice Screens in the Context of the Digital Markets Act*, ottobre 2023, *https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-132_Examining_the_Design_of_Choice_Screens_in_the_Context_of_the_Digital_Markets_Act.pdf* e in dottrina A. Fletcher, Z. Vasas, *Implementing the DMA: The role of behavioural insights*, in *Journal of European Competition Law & Practice*, Vol. 15, Issue 7, ottobre 2024, p. 456 ss.

LAVINIA DEL CORONA

# L'ACCENTRAMENTO DI FUNZIONI DI ESECUZIONE NORMATIVA E AMMINISTRATIVA NELLA SOCIETÀ DIGITALE: IL RUOLO DELLA COMMISSIONE EUROPEA



## 1. *La particolare esigenza di accentramento nella transizione digitale*

La disciplina della società digitale è divenuta uno dei principali ambiti di intervento normativo dell'UE[1]: negli ultimi anni si sono susseguiti, infatti, molti atti legislativi europei che in vario modo hanno introdotto regole per la società digitale, al fine ultimo di promuovere lo sviluppo tecnologico in Europa ma anche, e soprattutto, di garantire che i diritti fondamentali della persona siano garantiti nel mondo *online* allo stesso modo che nel mondo *off-line*[2].

L'esigenza di intervenire a tutela dei diritti fondamentali è sorta in ragione delle caratteristiche del tutto peculiari del mondo

[1] Per una ricostruzione dei principali interventi legislativi dell'UE di regolazione della società digitale si v. F. PIZZETTI, S. CALZOLAIO, E. LONGO, M. OROFINO, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024 e F. PIZZETTI, S. CALZOLAIO, E. LONGO, M. OROFINO, *La regolazione europea dell'intelligenza artificiale*, Giappichelli, Torino, 2025.

[2] La Comunicazione della Commissione europea COM(2020) 67 final, p. 10 ss., parla espressamente della costruzione di una «società aperta, democratica e sostenibile», in cui ciò che è illecito *offline* lo sia anche *online*.

digitale, in cui il potere economico è andato concentrandosi nelle mani di pochi operatori[3], che si sono trovati così nella condizione di esercitare poteri di fatto capaci di incidere anche profondamente sulla sfera pubblica e sui diritti fondamentali[4]. Una tale concentrazione di potere economico è stata possibile per ragioni di diverso tipo, prima fra tutte la sostanziale inefficacia della tradizionale normativa antitrust basata sulla teoria del prezzo[5] in un mercato in cui gli operatori offrono spesso prestazioni gratuitamente[6], potendo trarre beneficio economico in altri modi, in particolare grazie all'acquisizione dei dati personali degli utenti stessi[7].

I mercati digitali sono in tale modo venuti a caratterizzarsi per la presenza di monopoli e oligopoli privati dotati di un potere d'azione tale da essere capaci di pregiudicare fondamentali diritti e libertà delle persone, quali la libertà di espressione, di informazione e la riservatezza degli utenti. L'imposizione di limiti allo strapotere

[3] V., *ex multis*, L.M. Khan, *Amazon's Antitrust Paradox*, in *Yale Law Journal*, 2017, pp. 710-805; N. Srnicek, *Platform Capitalism*, Polity, 2017; T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*, Columbia Global Reports, New York, 2018.

[4] La letteratura sul tema è sterminata, si v., *ex multis*, T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation and the Hidden Decisions that Shape Social Media*, Yale University Press, 2018; K. Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, in *Harvard Law Review*, vol. 131, 2018, pp. 1598-1670; M. Moore, D. Tambini (a cura di), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, Oxford University Press, 2018; E. Douek, *The Rise of Content Cartels. The tech giants, monopoly power, and public discourse*, Knight First Amandment Institute at Columbia University, 2020. Nel panorama italiano si possono ricordare, *ex multis*, le riflessioni di M.R. Ferrarese, *Poteri nuovi*, Il Mulino, Bologna, 2021; L. Ammannati, *I «signori» nell'era dell'algoritmo*, in *Diritto Pubblico*, 2, 2021, pp. 381-413; M. Betzu, *Poteri pubblici e poteri privati nel mondo digitale*, in *Diritto pubblico*, 3, 2021, pp. 739-760; F. Paruzzo, *Sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Edizioni Scientifiche Italiane, Napoli, 2022; F. Balaguer, *La costituzione dell'algoritmo*, Mondadori, Milano, 2023; G.E. Vigevani, *Piattaforme digitali private, potere pubblico e libertà di espressione*, in *Diritto costituzionale*, 1, 2023, pp. 41-54.

[5] Sulla teoria del prezzo v. R.A. Posner, *The Chicago School of Antitrust Analysis*, in *University of Pennsylvania Law Review*, 127, 1979, p. 925 ss.

[6] Sul tema M. Betzu, *I poteri privati nella società digitale: oligopoli e antitrust*, cit., 3, 2021, p. 748 ss.

[7] Sui vantaggi economici che derivano dall'uso dei dati si v. E. Cremona, F. Laviola, V. Pagnanelli, *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Giappichelli, Torino, 2022.

degli operatori economici è divenuta, pertanto, di importanza cruciale per la tenuta dei sistemi democratici[8].

L'intervento pubblico necessario a tale fine è un intervento pubblico accentrato a livello sovra-statuale, in quanto la forza economica dei soggetti da regolare è tale per cui l'azione dei singoli Stati potrebbe ben poco: al potere economico delle strapotenze private occorre, quindi, contrappore il potere politico dell'Unione europea nel suo complesso[9].

Tale spinta accentratrice si è tradotta nella adozione a livello unionale in un ristretto lasso di tempo di molti atti legislativi – per lo più regolamenti – relativi alla regolazione della società digitale. Un primo importante passo si è avuto con l'approvazione del Regolamento (UE) 2016/679 sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, noto come *General Data Protection Regulation* (GDPR); a cui sono seguite molte altre iniziative, quale il Regolamento (UE) 2022/2065 relativo a un mercato unico dei servizi digitali, c.d. *Digital Services Act* (DSA); il Regolamento (UE) n. 2022/1925 relativo a mercati equi e contendibili nel settore digitale, c.d. *Digital Markets Act* (DMA); il Regolamento (UE) 2022/868 relativo alla *governance* europea dei dati, c.d. *Data Governance Act* (DGA); il Regolamento (UE) 2024/1689 sull'intelligenza artificiale, c.d. *AI Act*; il Regolamento (UE) 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo, c.d. *Data Act*; il Regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari, c.d. *European Health Data Space* (EHDS).

[8] È divenuta molto diffusa l'espressione "costituzionalismo digitale", utilizzata per indicare l'applicazione dei principi del costituzionalismo alla società digitale. Si v. D. Redeker, L. Gill, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, in *International Communication Gazette*, 4, 2018, pp. 302-319; O. Pollicino, *Judicial Protection of Fundamental Rights on the Internet. A Road Towards Digital Constitutionalism?*, Hart, 2021, p. 184 ss.; G. De Gregorio, *The Rise of Digital Constitutionalism in the European Union*, in *International Journal of Constitutional Law*, 1, 2021, pp. 41-70; E. Celeste, *Costituzionalismo digitale e piattaforme: verso una costituzionalizzazione della* lex digitalis, in *ComunicazionePuntoDoc*, 25, 2021, pp. 105-118.

[9] In tale senso E. Bruti Liberati, *Poteri privati e nuova regolazione pubblica*, in *Diritto pubblico*, 1, 2023, p. 297.

Ciò che nel presente lavoro si intende analizzare ed evidenziare è come ad un tale accentramento della disciplina legislativa a livello UE stia corrispondendo anche un accentramento delle funzioni di esecuzione normativa e amministrativa, che risultano essere in vario modo sottratte, *in toto* o in parte, agli Stati membri. Si osserverà, inoltre, come sempre più di frequente a tale sottrazione agli Stati membri stia corrispondendo l'attribuzione delle relative funzioni in capo alla Commissione europea, che vede dunque molto ampliate le proprie competenze normative e amministrative.

## 2. *L'accentramento di funzioni di esecuzione normativa*

### 2.1. *Il rinvio agli atti normativi della Commissione europea*

È da considerarsi come rispetto alla regolamentazione del settore digitale, oltre alla sopradescritta esigenza di accentramento, sussista anche una particolare esigenza di flessibilità normativa. Si tratta, infatti, di un settore fortemente esposto alla evoluzione tecnologica, per cui una normativa rigida, che non può essere agevolmente aggiornata, può facilmente divenire obsoleta. Da questo punto di vista l'ingente opera di regolamentazione posta in essere a livello europeo si espone alla critica di volere disciplinare un fenomeno in continua evoluzione tramite norme destinate a divenire in poco tempo inadeguate.

Sul punto, tuttavia, come osservato da attenta dottrina, il problema non pare essere il fatto in sé della previsione di regole giuridiche relative al digitale ma, piuttosto, quello di giungere in alcuni casi a disciplinare con fonte primaria – dunque dotata di particolare rigidità – anche aspetti di estremo dettaglio[10]. La particolare esigenza di flessibilità dovrebbe infatti portare a cercare un giusto equilibrio tra fonti primarie e secondarie: con la fonte primaria, più rigida, sarebbe bene porre in essere una disciplina di principio capace di adattarsi alla evoluzione della tecnica, mentre gli aspetti di dettaglio, che più facilmente possono divenire obsoleti, richiede-

[10] In tale senso A. IANNUZZI, *Le fonti del diritto per la disciplina della società digitale*, in F. PIZZETTI, S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea della società digitale*, cit., p. 20.

rebbero una regolamentazione con fonti più flessibili, che consentano di operare il costante aggiornamento reso necessario dalla rapida evoluzione tecnologica.

Considerato che all'esigenza di flessibilità si accompagna quella, di cui si è detto sopra, di accentramento dell'intervento pubblico, si capisce perché sia particolarmente auspicabile il ricorso a fonti secondarie elaborate a livello unionale. Vanno proprio in questo senso i molti rinvii agli atti delegati e agli atti esecutivi della Commissione europea che si rinvengono nei principali atti legislativi dell'UE di regolazione della società digitale.

Si tratta di deroghe alla regola generale per cui l'attuazione degli atti legislativi dell'UE dovrebbe spettare agli Stati membri, che trova riscontro all'art. 291 TFUE, ai sensi del quale gli Stati membri adottano «tutte le misure di diritto interno necessarie per l'attuazione degli atti giuridicamente vincolanti dell'Unione». La possibilità di discostarsi da tale regola è, d'altronde, riconosciuta dallo stesso art. 291 TFUE, il cui secondo paragrafo prevede che «allorché sono necessarie condizioni uniformi di esecuzione degli atti giuridicamente vincolanti dell'Unione» questi possano conferire alla Commissione il potere di adottare atti esecutivi. Inoltre, all'art. 290 TFUE è previsto che Consiglio e Parlamento con un atto legislativo possano «delegare alla Commissione il potere di adottare atti non legislativi di portata generale che integrano o modificano determinati elementi non essenziali dell'atto legislativo»[11]. La previsione di atti esecutivi e atti delegati della Commissione stempera, dunque, la regola generale per cui l'elaborazione della normativa secondaria spetterebbe agli Stati membri e consente una maggiore articolazione del sistema delle fonti dell'Unione europea.

Rispetto al rinvio agli atti delegati della Commissione europea, si può ricordare – ma gli esempi sarebbero molti – l'*AI Act*, in cui i rinvii agli atti delegati della Commissione sono molti e relativi ad

[11] Sugli atti delegati ed esecutivi della Commissione europea si v. P.P. Craig, *Delegated Acts, Implementing Acts and the New Comitology Regulation*, in *European Law Review*, vol. 36, 2011, pp. 671-687; L. De Lucia, B. Marchetti (a cura di), *L'amministrazione europea e le sue regole*, Il Mulino, Bologna, 2015, pp. 80-81; A. Turk, *Legislative, delegated acts, comitology and interinstitutional conundrum in EU law - configuring EU normative spaces*, in *European Law Journal*, 2021, pp. 1-14.

aspetti fondamentali per l'applicazione del Regolamento in questione. L'art. 11 del Regolamento, ad esempio, conferisce alla Commissione il potere di: i) adottare atti delegati al fine di modificare l'elenco delle tecniche e degli approcci di cui all'allegato I, per aggiornare tale elenco agli sviluppi tecnologici e di mercato sulla base di caratteristiche simili alle tecniche e agli approcci ivi elencati (art. 4); ii) di modificare l'allegato III aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio; iii) di modificare l'allegato IV ove necessario per garantire che, alla luce del progresso tecnico, la documentazione tecnica fornisca tutte le informazioni necessarie per valutare la conformità del sistema ai requisiti di cui al presente capo[12].

La tendenza a fare ricorso ai poteri normativi della Commissione europea ha raggiunto probabilmente l'apice nel Regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari.

Nel Regolamento in questione si rinvia in due punti agli atti delegati della Commissione europea, accompagnando tali previsioni con una dettagliata disciplina, di cui all'art. 97, dei tempi e dei limiti di esercizio di tali deleghe, con poteri di revoca e di controllo in capo al Parlamento e al Consiglio dell'UE. Ma soprattutto, nel Regolamento vi è un massiccio rinvio agli atti esecutivi della Commissione europea, specialmente per la definizione delle specifiche tecniche.

Tale accentramento di funzioni normative in capo alla Commissione europea ha suscitato la preoccupazione di parte della dottrina, con riferimento al pericolo che in tale modo scelte che implicano l'esercizio di discrezionalità politica siano rimesse ad un organo – la Commissione europea – che sarebbe privo della necessaria legittimazione democratica[13].

---

[12] Sui rinvii agli atti delegati della Commissione europea nell'*AI Act* si v. M. Ebers, *Truly Risk-Based Regulation of Artificial Intelligence - How to Implement the EU's AI Act*, in *SSRN*, 2024, p. 23 ss. (pp. 1-31); S. Greenstein, M. Zamboni, *Navigating the legislative dilemma: evaluating the EU AI Act's approach to regulating emerging technologies*, in *The Theory and Practice of Legislation*, 2025, p. 15 ss. (1-41); S. Calzolaio, *Autorità, governo, attuazione dell'AI Act*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, in *La regolazione dell'intelligenza artificiale*, cit., p. 148.

[13] In tale senso O. Pollicino, *Regolazione e innovazione tecnologica nell'"ordinamento della rete"*, in *Rivista AIC*, 2, 2025, p. 127.

Tuttavia, la Commissione europea, specie a seguito delle modifiche apportate dal Trattato di Lisbona, risulta avere acquisito natura politica e fondare la propria legittimazione democratica, sebbene indiretta, nel rapporto di fiducia che la lega al Parlamento europeo. Ciò che pare importante, al fine del rispetto del principio di separazione dei poteri e di legalità in senso sostanziale, non sembra, quindi, essere tanto evitare in assoluto che ad essa siano attribuite funzioni normative che richiedono l'esercizio di discrezionalità politica e non meramente tecnica, quanto, piuttosto, che a una tale attribuzione, specie laddove riguardi materie in cui sono coinvolti diritti fondamentali, si accompagnino specifiche indicazioni nell'atto legislativo in ordine all'oggetto, ai principi e ai criteri direttivi cui la Commissione deve attenersi.

### 2.2. *Gli atti di autoregolazione e di co-regolazione*

È però da considerarsi come la definizione di buona parte delle regole utili, o addirittura necessarie, per l'attuazione della disciplina generale stabilita negli atti legislativi UE per la transizione digitale continui ad essere effettuata, in tutto o in parte, da soggetti privati, che spesso risultano essere gli unici detentori delle conoscenze tecniche necessarie per l'esecuzione delle regole generali contenute negli atti legislativi UE[14]. Ciò avviene, in particolare, tramite l'attività di "autoregolazione" – laddove l'elaborazione delle regole è effettuata in autonomia dai privati – oppure tramite meccanismi di "co-regolazione" – che prevedono l'interazione tra pubblico e privato nella elaborazione della regola[15].

---

[14] Il tema è stato affrontato da G. De Minico, *Unione europea, mercato, tecnica* (versione provvisoria), Relazione al Convegno annuale dell'Associazione Italiana Costituzionalisti, Torino, 10-11 novembre 2025, pp. 1-50.

[15] Per un approfondimento sul tema si v. O. Pollicino, *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione online*, in *Rivista trimestrale di diritto pubblico*, 2022, pp. 1049-1066; A. Iannuzzi, *Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione*, in *Bilancio comunità persona*, 2, 2023, pp. 91-107; G. De Minico, *Libertà Virtuali. Costituzione e Mercato*, Merita, Torino, 2024, pp. 72 ss.; E. Cocchiara, *La regolazione del digitale: tra self-regulation, codici di condotta ed authorities*, in *Nuove Autonomie*, 1, 2025, pp. 385-407. Sulla co-regolazione si segnala anche il fascicolo speciale n. 1 del 2024 di Osservatorio

Il diritto dell'UE attribuisce in vario modo rilevanza giuridica alle regole così prodotte, attraverso meccanismi che risultano spesso rispondenti tanto all'esigenza di garantire norme flessibili che a quella di uniformità della disciplina sull'intero territorio UE. Ricorrendo ai privati l'UE evita, infatti, di delegare l'elaborazione della disciplina di attuazione delle fonti primarie UE ai singoli Stati membri, e, quindi, il relativo rischio di frammentazione normativa. Il rinvio ai privati può, infatti, garantire l'uniformità della disciplina sul territorio UE ove, come sempre più spesso accade, sia accompagnato dalla previsione di sistemi di orientamento e controllo da parte del soggetto pubblico accentrati a livello UE. Un accentramento che tende a determinare l'attribuzione di funzioni in capo alla Commissione europea, la quale, sebbene non elabori direttamente tali norme, si trova a svolgere un ruolo di rilievo nel procedimento relativo alla loro produzione.

Ciò vale in speciale modo con riferimento alle norme tecniche armonizzate, ossia norme tecniche rispetto alle quali il soggetto pubblico ha un ruolo di particolare rilievo e che, pertanto, sembrano uscire dalla logica della autoregolazione per avvicinarsi a quella della co-regolazione[16]. Le norme armonizzate sono adottate dagli Organismi di normazione europea su mandato della Commissione europea ai sensi di quanto previsto dal Regolamento (UE) 1025/2012 sulla normazione tecnica[17]. Al particolare ruolo del soggetto pubblico si associa, inoltre, una forza quasi vincolante delle norme stesse, grazie all'operare del meccanismo della "presunzione di conformità", in forza del quale chi aderisce alle norme tecniche

---

sulle fonti che raccoglie gli Atti del Convegno finale del Progetto PRIN 2017 Self- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law (SE.CO.R.E TECH) tenutosi a Firenze l'8 e 9 febbraio 2024.

[16] Sul confine labile tra autoregolazione e co-regolazione si v. G. Pistorio, *La co-regolazione nell'ecosistema digitale tra etero-regolazione e auto-regolazione. Questioni definitorie*, in *Osservatorio sulle fonti*, 1, 2024, p. 150.

[17] Sul tema si v. A. Zei, *Tecnica e diritto tra pubblico e privato*, Milano, 2008, p. 290 ss.; A. Iannuzzi, *Paradigmi normativi per la disciplina della tecnologia: auto-regolazione, co-regolazione ed etero-regolazione*, in *Bilancio comunità persona*, 2, 2023, p. 97 ss. Per una approfondita analisi del più generale tema delle norme tecniche nell'ordinamento interno e dell'Unione europea si v. A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Editoriale scientifica, Napoli, 2018.

armonizzate si presume avere tenuto un comportamento conforme agli obblighi di legge[18].

I rinvii alle norme armonizzate negli atti legislativi che regolano la società digitale sono molti. Si può ricordare il *Data Act*, dove, all'art. 33, si prevede che siano avanzate richieste di norme armonizzate in materia di interoperabilità dei dati, dei meccanismi e servizi di condivisione dei dati nonché degli spazi comuni europei di dati; il DSA, che, all'art. 44, prevede che la Commissione promuova l'adozione di norme tecniche e il loro aggiornamento rispetto a una serie di importanti tematiche; e l'*AI Act*, in cui, all'art. 40, si prevede che la Commissione presenti richieste di normazione riguardanti i requisiti dei sistemi di IA ad alto rischio e, se del caso, gli obblighi dei fornitori di IA per finalità generali.

Un ulteriore ricorso all'opera dei privati da parte degli atti legislativi che regolano la società digitale si ha per effetto del rinvio ai Codici di condotta, ossia codici di comportamento elaborati da soggetti privati nell'ambito, però, di un quadro normativo stabilito a livello legislativo.

Il ruolo del soggetto pubblico rispetto ai codici di condotta varia molto a seconda dei casi, potendosi esplicare in attività di promozione, controllo, pubblicità, e finanche recepimento[19].

Nel GDPR, ad esempio, si prevede un modello in cui il compito di promozione dei Codici di condotta è affidato a tutte le istituzioni pubbliche coinvolte, tanto nazionali che europee, mentre il controllo *ex post* è di competenza delle autorità di controllo nazionali[20]. Nel DSA si prevede, invece, che solo la Commissione europea e il Comitato europeo per i servizi digitali promuovano l'adozione dei Codici di condotta. Sono, inoltre, attribuiti alla Commissione particolari poteri che le consentono di concorrere alla elaborazione

---

[18] Si v. U. Carnevali, *La norma tecnica da regola di esperienza e norma giuridicamente rilevante. Ricognizione storica e sistemazione teorica. Ruolo dell'UNI e del CEI*, in *Responsabilità civile e previdenza*, 1997, p. 257 ss.; G.E. Bellisario, *La rilevanza del criterio presuntivo della conformità alle norme armonizzate*, in *Persona e mercato*, 2012, pp. 156-161.

[19] A. Simoncini, *La co-regolazione delle piattaforme digitali*, in *Rivista trimestrale di diritto pubblico*, 4, 2022, p. 1036.

[20] Art. 40 del Regolamento (UE) 2016/679.

del contenuto del Codice e di svolgere un controllo successivo alla sua adozione[21]. Nell'*AI Act* vi è poi un ulteriore modello, in cui molto più spazio è lasciato alla autonomia privata, poiché, infatti, i soggetti pubblici, in particolare l'Ufficio per l'IA e gli Stati membri, hanno il solo compito di promuovere l'adozione dei codici di condotta[22].

Il rinvio ai privati – per quanto orientati e controllati dal soggetto pubblico – per l'elaborazione di norme dall'evidente funzione pubblicistica presenta, tuttavia, non poche problematiche, non sempre facilmente risolvibili[23]. Si può, ad esempio, ricordare il complesso problema di garantire l'accessibilità delle norme armonizzate, a fronte della tendenziale conoscibilità degli standard tecnici da parte degli operatori economici solo dietro pagamento di un corrispettivo agli organismi di normazioni che li producono[24].

Non è, pertanto, da escludersi che in futuro possa giungersi, se non ad un superamento, quantomeno ad un ridimensionamento del ricorso a sistemi di autoregolazione o co-regolazione, con incremento, invece, della normativa secondaria prodotta dalle Istituzioni europee – ed in particolare dalla Commissione europea. La possibilità di sostituire le norme armonizzate con specifiche tecniche contenute negli atti esecutivi della Commissione europea risulta peraltro confermata da alcune recenti disposizioni degli atti legislativi che regolano la società digitale. Il riferimento è, in particolare, alle disposizioni che attribuiscono alla Commissione il compito di elaborare specifiche comuni laddove la norma armonizzata non sia di-

[21] Art. 45 del Regolamento (UE) 2022/2065. Sui codici di condotta nel DSA si v. R. Griffin, *Codes of Conduct in the Digital Services Act. Functions, Benefits & Concerns*, in *Technology and Regulation*, 2024, pp. 167-187.

[22] Art. 95 Regolamento (UE) 2024/1689. Sui codici di condotta nell'*AI Act* si v. P. Belotti, *I codici di condotta di cui alla Proposta di Regolamento UE sull'Intelligenza Artificiale. Ipotesi per un'applicazione dello* Human Rights-Based Approach, in *Rivista di Scienze Giuridiche, Scienze Cognitive ed Intelligenza Artificiale*, 2, 2022, pp. 50-69.

[23] Per una chiara ricostruzione delle diverse problematiche legate al rinvio alle norme tecniche si v. A. Iannuzzi, *Le fonti del diritto dell'Unione europea per la disciplina della società digitale*, in F. Pizzetti, S. Calzolaio, E. Longo, M. Orofino, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024, pp. 47 ss.

[24] Sul tema si è recentemente pronunciata la Corte di Giustizia affermando che qualora lo standard tecnico risponda ad interessi pubblici esso debba essere reso accessibile gratuitamente, Corte giust., 5 marzo 2024, causa C-588/21, Public.Resource.Org, Inc. e Right to Know CLG contro Commissione europea.

sponibile – perché, ad esempio, non ancora elaborata o perché la richiesta è stata respinta –[25], ma soprattutto al Regolamento sullo spazio europeo dei dati sanitari, in cui è stata compiuta la particolare scelta di rinviare direttamente alle specifiche tecniche che la Commissione europea elaborerà nei propri atti esecutivi piuttosto che alle norme armonizzate degli organismi di normazione.

Ciò che pare però ostare, quantomeno al momento, alla acquisizione da parte della Commissione europea di un ruolo generalizzato di tale tipo è la mancanza in capo alla stessa delle necessarie competenze tecniche e l'assenza di un apparato amministrativo europeo alle sue dipendenze sufficientemente sviluppato per potergliele fornire.

## 3. *L'accentramento delle funzioni amministrative*

Parallelamente all'accentramento riscontrato sia nella produzione normativa primaria sia in quella secondaria, si assiste anche a un rafforzamento delle competenze amministrative in capo alle Istituzioni europee, con un progressivo superamento della tradizionale impostazione fondata sul principio della cosiddetta "amministrazione indiretta", per cui di regola l'esecuzione del diritto dell'UE sarebbe rimessa alle autorità nazionali[26].

Le più recenti iniziative legislative europee in materia digitale hanno determinato una crescita significativa delle attività di amministrazione diretta dell'UE[27], contribuendo così al processo di for-

---

[25] In questo senso ad esempio l'art. 33, par. 5, del *Data Act* e l'*AI Act*. Sul tema si v. M. Orofino, *La regolazione dei modelli di IA per finalità generale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea dell'intelligenza artificiale*, cit., p. 105; E. Longo, *Le pratiche di IA vietate e i sistemi di IA ad alto rischio: metodi e strumenti per la società del "rischio digitale"*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La regolazione europea dell'intelligenza artificiale*, cit., p. 87.

[26] Su come tale regola originaria abbia subito nel tempo diverse eccezioni, con quindi avvio di un processo di costruzione e crescita della amministrazione europea si v. L. De Lucia, B. Marchetti (a cura di), *L'amministrazione europea e le sue regole*, Il Mulino, Bologna, 2015, p. 47.

[27] F. Pizzetti, *Introduzione alla regolazione europea della società digitale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea della società digitale*, cit., 2024, p. 4.

mazione di una amministrazione europea avente centro operativo nella Commissione europea[28].

Ripercorrendo le principali tappe che nell'ambito della transizione digitale hanno determinato tale processo, un primo passaggio rilevante è rappresentato dal GDPR, che ha introdotto un'evoluzione strutturale: oltre a imporre agli Stati membri la creazione di autorità nazionali indipendenti, esso ha istituito il Comitato europeo per la protezione dei dati, un'autorità indipendente europea con funzioni di coordinamento e indirizzo rispetto alle autorità indipendenti nazionali[29].

Se la previsione di autorità indipendenti nazionali non costituiva una vera novità, innovativo è stato invece l'inserimento di un organismo europeo di vertice, incaricato di garantire uniformità di applicazione e coerenza interpretativa. Il Comitato svolge, infatti, un ruolo di armonizzazione e risoluzione dei conflitti tra le autorità nazionali nell'ambito del cosiddetto "meccanismo di coerenza", nonché funzioni di orientamento tramite linee guida, pareri e criteri di certificazione, e di consulenza nei confronti della Commissione in materia di protezione dei dati personali[30].

Gli atti successivi nel campo della regolazione digitale hanno, inoltre, segnato un ulteriore passaggio: sempre più spesso le funzioni amministrative vengono attribuite direttamente alla Commissione, che vede così consolidarsi la propria posizione di vertice dell'amministrazione europea[31].

Nel *Digital Services Act* (DSA), ad esempio, pur prevedendosi la costituzione di autorità nazionali indipendenti, la Commissione è investita di poteri diretti di vigilanza e attuazione della normativa,

---

[28] L. De Lucia, B. Marchetti (a cura di), *L'amministrazione europea*, cit., p. 47.

[29] S. Calzolaio, *Autorità indipendenti e di governo della società digitale*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea della società digitale*, cit., p. 86 ss.

[30] Artt. 63-65 del GDPR. Sull'accentramento amministrativo nel GDPR si v. F.B. Bastos, P. Palka, *Is Centralised General Data Protection Regulation Enforcement a Constitutional Necessity?*, in *European Constitutional Law Review*, vol. 19, 3, 2023, pp. 487-517.

[31] Sul tema L. Torchia, *I poteri di vigilanza, controllo e sanzionatori nella regolazione europea della trasformazione digitale*, in *Rivista Trimestrale di Diritto Pubblico*, 2022, pp. 1101 ss.; S. Calzolaio, *Autorità indipendenti*, cit., p. 96.

in particolare in relazione alle piattaforme di grandi dimensioni[32]. Essa dispone di competenze esclusive per l'attuazione di specifiche disposizioni del Regolamento, di poteri di controllo sui codici di condotta e può intervenire autonomamente in caso di violazioni gravi o reiterate.

L'accentramento amministrativo ha però raggiunto il massimo livello nel *Digital Markets Act* (DMA), dove la Commissione è individuata come l'unica autorità competente per l'applicazione del regolamento. A essa spettano la designazione dei *gatekeeper*, il monitoraggio delle loro condotte e l'irrogazione delle sanzioni[33].

Anche nel Regolamento sull'intelligenza artificiale (*AI Act*) permane un ruolo di primo piano della Commissione, che esercita poteri di controllo sulle autorità nazionali di notifica e competenze esclusive di vigilanza e sanzione per i modelli di IA ad alto rischio[34].

Analogo accentramento si riscontra nel Regolamento sullo spazio europeo dei dati sanitari (EHDS), che assegna alla Commissione rilevanti compiti di monitoraggio e verifica dell'attuazione da parte degli Stati membri, oltre alla gestione diretta delle infrastrutture e dei servizi centrali necessari al funzionamento dello spazio europeo dei dati sanitari, tra cui la piattaforma MyHealth@EU.

In linea generale, si può osservare che il livello di accentramento amministrativo cresce proporzionalmente alle dimensioni e alla forza economica dei soggetti regolati[35]: non sorprende quindi

---

[32] P. Mattioli, *Navigating the Complexities of the DSA's Enforcement Framework: Sincere Cooperation in Action?*, in *Utrecht Law Review*, 2025, pp. 2-17; R. Sabia, *L'enforcement pubblico del Digital Services Act tra Stati membri e Commissione europea: implementazione, monitoraggio e sanzioni*, in *Media Laws*, pp. 92 ss.

[33] G. Giordano, *Il* Digital Markets Act *e la centralizzazione dei poteri in capo alla Commissione europea: quale ruolo per le Autorità antitrust nazionali?*, in *Comparazione e diritto civile*, 3, 2022; M. Orofino, *Il* Digital Market Act*: una regolazione asimmetrica a cavallo tra diritto alla protezione dei dati e diritto antitrust*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, *La Regolazione società digitale*, cit., p. 168; A. Ribera Martínez, *The decentralisation of the DMA's Enforcement System*, in *GRUR International*, vol. 73, Issue 12, 2024, pp. 1111-1127.

[34] F. Ferri, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in *Quaderni AISDUE*, 2, 2024, pp. 1-20.

[35] M. Eifert, A. Metzger, H. Schweitzer, G. Wagner, *Taming the Giants: the DMA/DSA Package*, in *CMLR*, 4, 2021, pp. 987-1028.

che esso raggiunga il suo apice nel DMA, che ha come destinatari i principali attori del mercato digitale.

Tale trasferimento di funzioni amministrative dirette alla Commissione solleva, tuttavia, alcune criticità, soprattutto in relazione alla sussistenza in capo alla stessa delle competenze tecniche necessarie. Per questo motivo, accanto alla Commissione, gli atti europei hanno previsto la creazione di diversi organismi consultivi e di supporto – quali il Comitato europeo per la protezione dei dati, il Comitato europeo per l'innovazione in materia di dati, il Comitato europeo per i servizi digitali, il Consiglio europeo per l'IA e il Comitato dello spazio europeo dei dati sanitari – destinati a coadiuvarla nell'esercizio delle sue funzioni.

Particolarmente significativa in tal senso è l'istituzione dell'Ufficio per l'IA, incardinato all'interno della Commissione stessa, che, ai sensi dell'art. 3 dell'*AI Act*, costituisce «la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024». L'Ufficio in questione è stato pensato, dunque, come una articolazione interna della Commissione europea, a cui risulta legato da un rapporto di immedesimazione organica, in quanto, sempre ai sensi dell'art. 3 del Regolamento, «I riferimenti all'ufficio per l'IA (…) si intendono fatti alla Commissione». È di rilievo, in particolare, che molte funzioni di amministrazione attiva siano attribuite dall'*AI Act* direttamente all'Ufficio per l'IA che opera alle dipendenze della Commissione ma che risulta essere dotato di un certo grado di autonomia rispetto ad essa. Si tratta di un dato importante perché, a bene vedere, in esso potrebbe ravvisarsi l'avvio, sebbene in fase ancora embrionale, di un processo di costruzione di un apparato amministrativo alle dipendenze della Commissione europea, deputato allo svolgimento della funzione amministrativa[36].

[36] F. Pizzetti, *Il regolamento europeo della IA come parte integrante della normativa UE per il decennio digitale europeo 2030*, in F. Pizzetti, S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino (a cura di), *La regolazione europea dell'intelligenza artificiale nella società digitale*, cit., p. 5, secondo il quale l'istituzione di tale Ufficio sarebbe indicativa dell'affermarsi di un «nuovo paradigma» che richiede la istituzione di

Si tratterebbe di una evoluzione importante per garantire la competenza tecnica necessaria per lo svolgimento delle funzioni amministrative, ma anche la necessaria imparzialità dell'azione amministrativa. Una problematica insita nella attribuzione diretta in capo alla Commissione europea – organo che esercita il potere esecutivo dell'UE – di funzioni di amministrazione attiva potrebbe infatti ravvisarsi nel rischio che l'imparzialità della funzione amministrativa sia compromessa dal carattere politico della Commissione. La creazione di apparati amministrativi che, seppure alle dipendenze della Commissione, siano dotati di un certo grado di autonomia rispetto ad essa, potrebbe invece consentire, sul modello degli apparati ministeriali presenti nelle amministrazioni statali, di meglio distinguere la funzione amministrativa da quella esecutiva.

## 4. *Considerazioni conclusive*

Alla luce di quanto sino a qui osservato pare importante in conclusione porre in evidenza come l'accentramento in capo alla Commissione europea di funzioni relative alla esecuzione normativa e amministrativa della disciplina legislativa UE sulla società digitale incida di fatto sul processo di integrazione europea, in particolare rafforzando il ruolo della Commissione come soggetto titolare del potere esecutivo dell'UE. Nella tensione da sempre presente tra il modello federale e il modello dell'organizzazione internazionale, il rafforzamento di una Istituzione – la Commissione – che risponde chiaramente alla logica confederativa, spinge, dunque, nel senso della prevalenza del primo modello a discapito dell'altro e sembra, così, determinare alcuni importanti passi in avanti nel percorso di affermazione dell'Unione europea come Stato federale.

Tale rafforzamento, tuttavia, non è privo di criticità.

Si è, ad esempio, visto come sia importante che gli atti legislativi delimitino e orientino il potere normativo conferito alla Commissione e che sia implementato un apparato amministrativo capace

---

nuovi uffici all'interno della Commissione europea, che la supportino nello svolgimento dei suoi ruoli di vigilanza e di nuove forme di cooperazione da parte dei rappresentanti degli Stati membri all'attività di vigilanza della Commissione.

di fornire adeguato supporto alla Commissione per l'espletamento delle sue funzioni amministrative.

Più in generale, si pone il problema di evitare una problematica commistione di funzioni in capo alla Commissione europea. L'affermarsi della stessa come esecutivo dell'UE rende opportuna, in particolare, una complessiva rimeditazione del ruolo e delle prerogative delle Istituzioni europee, che vada a bilanciare le altrimenti eccessive funzioni della Commissione. L'acquisizione di funzioni esecutive da parte della Commissione rende, ad esempio, sempre più difficilmente giustificabile il suo essere, allo stesso tempo, l'unico soggetto titolare del potere di iniziativa legislativa. Così come si è visto che il suo affermarsi come organo titolare del potere esecutivo dell'UE rende problematico il fatto che alcune funzioni di amministrazione attiva siano attribuite direttamente ad essa e non invece a organi eventualmente operanti alle sue dipendenze ma dotati di margini di autonomia.

MARIA FRANCESCA DE TULLIO

# LA GEOPOLITICA DEI *BIG DATA* NEL REGIME EUROUNITARIO DELLE TELECOMUNICAZIONI: *COMPETITION LAW* E AUTODETERMINAZIONE INFORMATIVA



## 1. *Introduzione*

Il presente lavoro indaga come le preoccupazioni geopolitiche emergono nella regolazione eurounitaria e mutano l'equilibrio che la disciplina dei *big data* realizza tra innovazione, autodeterminazione informativa e *competition law*. Rispetto all'ampia dottrina che si è soffermata sul rapporto tra questi tre valori, questo breve contributo mira a tracciare l'*ubi consistam* della disciplina dei *big data* nelle telecomunicazioni, in un momento in cui le preoccupazioni tradizionali delle politiche digitali si intrecciano con la guerra in atto ai confini orientali dell'Unione.

La domanda di ricerca nasce dall'osservazione di un mutamento discorsivo dell'Unione, in cui la regolazione dei *big data* – un tempo dominata dal linguaggio del libero mercato – sembra aver integrato preoccupazioni extra economiche, incentrate sull'autonomia tecnologica e la *data sovereignty* come presidio della sicurezza interna ed esterna. Ci si interroga, dunque, sui mutamenti politico-giuridici sottostanti e/o conseguenti alla nuova retorica, tematizzando se e come il nuovo approccio cambi l'equilibrio tra i valori in gioco, ridefinendo tanto la disciplina dei diritti quanto il volto della

*competition law*. È sempre più chiaro, infatti, che quest'ultima integra aspetti non soltanto tecnico-economici, ma anche politico-valoriali. Per tale ragione, parte della dottrina ha spinto verso un'interpretazione costituzionalmente orientata di tale settore regolativo, che ruota attorno ai diritti umani.

Proprio sulla ridefinizione di questi valori si concentra questo scritto, che sarà articolato in tre momenti chiave.

Il paragrafo II mostra la natura strategica dei *big data*, che tocca diversi valori dell'ordinamento, talvolta in reciproco conflitto. In questa prima fase, l'analisi partirà dal modello tuttora dominante, che è il punto di partenza per osservare e valutare le successive innovazioni: un sistema che riconosce diritti esclusivi in capo a chi raccoglie e tratta in massa i dati degli utenti. A tali questioni non fa eccezione il campo delle telecomunicazioni, dove i dati sono usati per il miglioramento del servizio – ad esempio, con l'individuazione di malfunzionamenti o la creazione di offerte su misura – ma anche per la loro vendita e monetizzazione[1]. Tali informazioni – sebbene non includano, salvo eccezioni, i contenuti trasmessi – sono ricche di metadati circa l'identità dell'utente e le circostanze della comunicazione.

Il paragrafo III si sofferma su come i conflitti appena indicati siano stati nel tempo oggetto di diverse risposte regolatorie, con livelli variabili di connessione – almeno dichiarata – con le questioni geopolitiche e di sicurezza interna ed esterna dell'Unione. Il ragionamento dimostrerà come i *big data* siano parte integrante e cruciale – nonché concausa – di un cambiamento di paradigma regolatorio, che sotto la definizione di sovranità digitale ha progressivamente spostato l'asse – quantomeno discorsivo – dal libero mercato alla sicurezza nazionale. Si osserverà dunque come tali politiche abbiano cambiato il paradigma regolativo dominante: dall'assolutezza della proprietà a una strumentalità all'affermazione della sovranità dell'UE e degli Stati membri.

---

[1] M. Kaur, *Why is Big Data important in the Telecom industry?*, in *DatatoBiz.com*, in *https://www.datatobiz.com/blog/big-data-in-telecom-industry/#:~:text=Big*; M.Z. Kastouni, A.A. Lahcen, *Big Data Analytics in Telecommunications: Governance, Architecture and Use Cases*, in *Journal of King Saud University - Computer and Information Sciences*, 2020, pp. 4 ss.; Z. Wang, G. Wei, Y. Zhan, Y. Sun, *Big data in telecommunication operators: data, platform and practices*, in *Journal of Communications and Information Networks*, vol. 2(3), 2017, pp. 79-80.

Il paragrafo IV, infine, valuta avanzamenti e limiti di questo nuovo paradigma, evidenziando alcune possibili vie per un riequilibrio tra i valori in gioco, fondato su valori di uguaglianza e democrazia.

## 2. *I* big data *nelle telecomunicazioni. I valori in gioco*

Il primo passo del ragionamento è enucleare la 'posta in gioco' giuridico-valoriale dei *big data* nell'ordinamento UE, composta di obiettivi talora contrastanti tra loro, in rapporto mutevole con la *competition law*. Anche se questi conflitti e sinergie regolatori sono ben noti alla dottrina giuridica, si ritiene utile richiamarli qui brevemente in quanto sono al centro dei cambiamenti che avvengono nelle politiche eurounitarie.

### *A) L'innovazione tecnologica*

L'innovazione è il primo pilastro di questo ragionamento, in quanto proprio tale obiettivo legittima l'esistenza di diritti esclusivi in capo agli operatori rispetto ai *big data* raccolti dalle persone utenti.

Come è noto, l'economia digitale si basa ampiamente sull'acquisizione di simili dati, in occasione della fornitura del servizio o in cambio della stessa. Pur non essendo comprovata la natura proprietaria di tali diritti, essi condividono con il diritto di proprietà intellettuale la medesima giustificazione giuridica e buona parte delle facoltà connesse alla loro posizione soggettiva: quanto meno, il diritto di usare e trarre profitti dal bene, ma anche ampi – seppur non illimitati – poteri dispositivi[2]. Nel caso di un bene non rivale, come i dati, la proprietà non si giustifica sulla base della necessità di regolare l'appropriazione della risorsa, per evitare il suo esaurimento o possibili conflitti d'uso. Infatti, per definizione, tali beni possono essere goduti da più soggetti contemporaneamente, per cui

[2] T. Groza, B. Botero Arcila, *The New Law of the European Data Markets: Demystifying the European Data Strategy*, in *Global Jurist*, vol. 24(3), 2024, pp. 335 ss.; C. Ducuing, *Data as a Contested Commodity*, in *Global Jurist*, vol. 24(3), 2024, pp. 281 ss.

il diritto d'uso dell'uno non priva l'altro del suo analogo diritto. Piuttosto, il fondamento giuridico dei diritti esclusivi sui dati – esattamente come nel caso della proprietà immateriale – si basa sull'obiettivo politico-giuridico di sostenere l'innovazione: uno dei modi per incentivare i privati a impiegare risorse in ricerca e sviluppo è assicurare alle imprese un ritorno di investimento in termini di profitti derivati dalla somministrazione del servizio, che nel caso di Internet viene pagato in termini di dati, più che di remunerazione monetaria diretta.

Se si guarda al rapporto con altri diritti, bisogna tenere in considerazione almeno due fattori. Il primo è che l'attribuzione di diritti esclusivi non è l'unico modo possibile per incentivare la ricerca, la quale ben può essere sostenuta, ad esempio, con premi o investimenti *ad hoc*. Anzi, la previsione può rivelarsi addirittura controproducente in taluni casi, qualora si verifichi la c.d. *tragedy of anticommons*[3], per cui i beni immateriali sono sottoutilizzati in quanto soggetti a *enclosures*, con la rinuncia a una parte del loro potenziale di innovazione. Non a caso, si osserverà, proprio rispetto a questo punto l'Unione Europea ha mutato atteggiamento nel tempo, favorendo la condivisione dei dati invece che la loro concentrazioni nelle mani delle *corporation*. Il secondo fattore è che l'innovazione tecnologica è un valore-mezzo che deve essere letto alla luce del valore-fine: la tecnica realizza l'interesse generale non in astratto, ma nella misura in cui è concretamente orientata a questo fine. L'identificazione del valore-fine è particolarmente rilevante se si osserva il bilanciamento con altri valori, tutti connessi tra loro e legati intimamente alla sovranità: la sicurezza interna ed esterna, da un lato, e l'autonomia e autodeterminazione democratica, dall'altro.

### *B) La pubblica sicurezza*

La pubblica sicurezza come valore si pone in rapporto ambiguo con la proprietà dei dati, in quanto la raccolta in massa aumenta il numero di informazioni esposte, che possono essere con-

[3] F. Murray, S. Stern, *Do formal intellectual property rights hinder the free flow of scientific knowledge? An empirical test of the anti-commons hypothesis*, in *Journal of Economic Behaviour and Organizations*, vol. 63(4), 2007.

sultate per la prevenzione dei rischi interni ed esterni. Di conseguenza, i modelli *data driven* possono rivelarsi utili anche per tali esigenze di tutela. Tuttavia, ciò non esclude la presenza di altre contraddizioni: le esigenze di sicurezza possono imporre limiti – come la localizzazione o la conservazione dei dati – potenzialmente onerosi per le imprese, specie quelle emergenti, soprattutto quando esse si devono adattare alle differenze regolative tra Stati, allorché il servizio che loro forniscono travalica naturalmente i confini. Inoltre, le imprese hanno lamentato un danno di immagine in determinate fasi storiche, allorché la sorveglianza governativa e di *intelligence* ha causato la perdita di fiducia da parte del grande pubblico rispetto ai medesimi attori della rete. Tali frizioni possono dare luogo a risposte diverse da parte del potere pubblico, spesso combinate tra loro: l'opzione *command and control* e quella di costruzione del consenso all'interno del settore.

Il tema è ben esemplificato dalla vicenda della direttiva *Data Retention*[4], che imponeva un duplice obbligo agli operatori di telecomunicazioni: la conservazione in massa dei metadati sulle comunicazioni e la loro messa a disposizione per l'accesso all'autorità in caso di necessità. Come è noto, la Direttiva è stata annullata dalla Corte di Giustizia per la portata sproporzionata della sorveglianza realizzata[5], ma non aveva mancato di creare malcontento anche tra gli operatori di telecomunicazioni, che si sono visti imporre responsabilità onerose dalla normativa[6]. Oggi, in mancanza di una nuova

---

[4] *Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE*, in *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:IT:PDF.*

[5] Corte di Giustizia dell'Unione Europea - Grande Sezione, *Digital Rights Ireland Ltd c. Ireland*, cause riunite C-293/12 e C-594/12, 8 aprile 2014, in *http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dbcd805c70edfe45d48ed4fd48d0b7dd70.e34KaxiLc3qMb40Rch0SaxuNaNf0?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=205128.*

[6] Commissione per le libertà civili, la giustizia e gli affari interni, *Relazione sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE* (COM(2005)0438 - C6 0293/2005 - 2005/0182(COD)), in *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//*

disciplina armonizzata, i medesimi attori si vedono costretti ad adempiere al *patchwork* delle diverse regolazioni nazionali che l'UE si appresta a gestire in modo unitario ricorrendo a un procedimento consensuale.

### *C) L'autodeterminazione informativa*

Naturalmente, la raccolta massiva dei dati riguarda anche l'autodeterminazione informativa, come diritto fondamentale e sovraordinato alle libertà economiche[7], che assicura a ciascuna persona il controllo sulle proprie informazioni personali[8].

Come è noto, una delle sfide regolatorie poste dai *big data* è l'ampio spazio lasciato al consenso della persona interessata, che a oggi appare una garanzia debole rispetto allo sfruttamento economico dei dati. Infatti, da un lato si affida la tutela della *privacy* a una negoziazione iniqua tra consumatore e imprenditore, dall'altro non si tiene adeguatamente conto dell'interesse collettivo all'autodeterminazione informativa. Questo interesse può giustificare un più alto livello di indisponibilità dei dati, nonché la previsione di modalità per la negoziazione collettiva su tali interessi[9], a tutela dell'uguaglianza sostanziale e degli interessi collettivi legati all'autodeterminazione informativa.

L'uguaglianza viene in rilievo nella misura in cui la vera autodeterminazione è possibile solo quando la persona è libera dai bi-

---

*NONSGML+REPORT+A6-2005-0365+0+DOC+WORD+V0//IT*, *Parere della Commissione per l'industria, la ricerca e l'energia*.

[7] *Google Spain SL, Google Inc. contro Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, 13/5/2014, in *http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&from=HR*, punti 97 e 99.

[8] Il punto di riferimento cardine, nel caso dell'Unione Europea, è evidentemente il c.d. Regolamento Generale sulla Protezione dei Dati: *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 (regolamento generale sulla protezione dei dati)*. Sull'argomento, si veda il contributo di M. Orofino in questo *Volume*.

[9] A. Anciaux, J. Farchy, *Données personnelles et droit de propriété: quatre chantiers et un enterrement*, in *Revue internationale de droit économique*, vol. 3/2015, in *http://www.cairn.info/revue-internationale-de-droit-economique-2015-3-page-307.htm*, p. 326.

sogni economici[10]. Al contrario, potrebbero esserci cessioni solo apparentemente volontarie, dettate in realtà da uno stato di necessità[11]. Ad esempio, chi non ha altri mezzi di sussistenza è più disponibile a ricorrere alla vendita di organi; allo stesso modo, le rinunce e le transazioni sui diritti derivanti dal rapporto di lavoro sono sospette, perché potrebbero essere il risultato della situazione di debolezza in cui si trova il dipendente rispetto al datore di lavoro. Per questo motivo tali accordi sono regolamentati in modo restrittivo: si tratta di una compressione formale della libertà volta a una sua maggiore attuazione sostanziale. Nello stesso senso, potrebbe essere giustificata una maggiore indisponibilità dei dati personali.

È poco contestato il fatto che in molte situazioni della vita quotidiana, e oggi anche su Internet, una persona comune non abbia una reale possibilità di scelta quando si tratta di decidere se cedere o meno i propri dati, perché il consenso è spesso l'unico modo per accedere ai servizi necessari alla vita quotidiana[12]. Lo stesso legislatore europeo del GDPR ha preso in considerazione questa ipotesi e ha previsto garanzie per il consenso al trattamento dei dati personali, sebbene insufficienti in base a quanto qui argomentato.

Il secondo interesse pubblico che legittima e impone una maggiore indisponibilità dei dati personali è l'autodeterminazione informativa della comunità. È indiscutibile che le posizioni giuridiche individuali possano essere sacrificate a favore di un interesse collettivo tutelato dalla Costituzione, purché siano rispettati i principi di ragionevolezza e proporzionalità e l'intangibilità del loro 'nucleo duro'. A volte, come in questo caso, un diritto può essere garantito agli individui solo se è garantito alla società nel suo complesso: per

[10] È stato sottolineato che i limiti ai contratti assumono un'importanza crescente laddove si verificano crescenti violazioni dei diritti da parte di privati cittadini, i quali in alcuni casi sono in grado di sviluppare, attraverso contrattazioni standardizzate, vere e proprie regole generali sul bilanciamento dei diritti: G. RESTA, *La disponibilità dei diritti fondamentali e i limiti della dignità*, cit., pp. 804-806; M.J. RADIN, *Regulation by Contract, Regulation by Machine*, *Stanford Public Law and Legal Theory Working Paper Series - Research Paper* No. 92, April 2004, pp. 3-7.

[11] M.J. RADIN, *Market-inalienability*, in *Harv. Law Rev.*, vol. 100(8), 1987, pp. 1909-1913. Cfr., anche se rispetto all'azione coattiva della pubblica autorità: *Cases of De Wilde, Ooms and Versyp ("vagrancy") v. Belgium (merits)*, Application no. 2832/66; 2835/66; 2899/66, 18/6/1971, in *http://www.univie.ac.at/bimtor/dateien/ecthr_1971_dewilde_ vs_belgium.doc*, § 65; *Case of Deweer v. Belgium*, cit., §§ 49-54.

quanto riguarda le malattie infettive, ad esempio, bastano poche persone malate perché la malattia si diffonda. Anche la libertà di informazione ha valore solo se è protetta per tutti: il suo scopo ultimo è quello di garantire un dialogo tra una pluralità di voci, in modo che ciascuno possa arricchirsi del contributo degli altri.

In tal senso, oggi anche la *privacy* è un interesse collettivo oltre che individuale: *rectius*, essa può essere tutelata per le singole persone solo se garantita a tutte, poiché l'atto dispositivo di una ha effetti negativi anche sulle altre[13]. Ci sono almeno tre argomenti a sostegno di questa affermazione, i quali giustificano quindi una regolamentazione generale che limiti i diritti degli individui.

Il primo argomento risiede nel fatto che ogni nuovo consenso al trattamento dei dati contribuisce al dominio di pochi centri di potere socio-economico[14] che si pongono in concorrenza sleale con la sovranità popolare. Un secondo argomento che manifesta una dimensione collettiva della *privacy* è legato al pericolo di discriminazione insito nel data mining, che se dovesse concretizzarsi avrebbe ripercussioni sulla società nel suo complesso. «L'uso della profilazione algoritmica per l'allocazione delle risorse è, in un certo senso, intrinsecamente discriminatorio: la profilazione avviene quando le persone interessate vengono raggruppati in categorie in base a varie variabili e le decisioni vengono prese sulla base dell'appartenenza dei soggetti a gruppi così definiti»[15].

---

[12] B.W. Schermer, B. Custers, S. van der Hof, *The Crisis of Consent*, cit., 11-12; P.M. Schwartz, *Internet Privacy and the State*, in *Conn. L. Rev.*, 1999-2000, pp. 32; V. Peugeot, *Données personnelles: sortir des injonctions contradictoires*, in *Vecam.org*, 13/4/2014, in *http://vecam.org/archives/article1289.html*.

[13] In questo senso, D.D. Hirsch paragona le violazioni della *privacy* ai danni ambientali: l'azienda danneggia un bene comune senza sostenerne i costi: *Is Privacy Regulation the Environmental Law of the Information Age?*, in K. Strandburg, D. Stan Raicu (eds.), *Privacy and Technologies of Identity: a Cross-disciplinary Conversation*, New York, 2005, § 2.

[14] E. Morozov, *The Real Privacy Problem*, in *MITTechnologyReview.com*, 22.10.2013, in *http://www.technologyreview.com/featuredstory/520426/the-real-privacy-problem/*.

[15] B. Goodman, S. Flaxman, *EU regulations on algorithmic decision-making and a "right to explanation"*, Paper presented at the *ICML Workshop on Human Interpretability in Machine Learning*, 28/6/2016, in *http://arxiv.org/pdf/1606.08813v1.pdf*, pp. 27.

Un terzo e ultimo argomento è di natura più strutturale: il risultato del *data mining* non deriva dall'analisi di dati isolati, bensì da un'indagine probabilistica che nasce dall'incrocio e dalla combinazione del maggior numero possibile di informazioni, anche provenienti da soggetti diversi. Infatti, le scelte basate sui dati non vengono effettuate sull'individuo, ma sul gruppo in cui l'individuo è inserito secondo le statistiche[16]. Ogni persona ha quindi un interesse giuridicamente tutelato a sapere quali e quanti dati vengono divulgati dagli altri e alla correttezza di tali informazioni, poiché anche le decisioni che riguardano la persona stessa vengono prese sulla base di questi parametri[17].

*D*) *La* competition

La *competition* ha assunto nel tempo un rapporto variabile rispetto ai valori sopra esposti, inevitabilmente influenzata dagli obiettivi di politica economica che il regolatore ha inteso realizzare.

Rispetto ai *big data*, oggi è in atto un progressivo mutamento della regolazione concorrenziale. In una prima fase, l'obiettivo prevalente è stato la libera circolazione, che tuttavia ha compromesso il gioco competitivo, a causa delle specificità dei mercati in questione[18]. Infatti, le piattaforme operano su un mercato 'a due versanti': da un lato, forniscono un servizio – apparentemente gratuito – in cambio della cessione di dati sull'identità e il comportamento dell'utente, dall'altro lato profittano di questi dati grazie alla vendita di servizi pubblicitari mirati o la creazione di intelligenze artificiali. Tali meccanismi favoriscono sistematicamente chi è già forte[19],

---

[16] A. Vedder, *Medical Data, New Information Technologies, and the Need for Normative Principles other than Privacy Rules*, in *https://pure.uvt.nl/portal/files/368983/Ucl2.pdf*, paper published in *Law Med*, n. 3, 2000, pp. 14-18.

[17] A. Mantelero, *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, in *Comp. L. & Sec. Rev.*, vol. 32(2), 2016, pp. 12-14.

[18] Sull'impatto dei *big data* sulla concorrenza: H. Kim, *Data Concentration and Competition in Digital Platforms*, KIEP Research Paper, World Economy Brief (WEB), 2024, 2.

[19] A. Macchiati, *I motori di ricerca su Internet e il mercato delle news*, in *Mercato concorrenza regole*, n. 3, 2010, p. 478; M.L. Wang, *The Market Reality for an Ailing Democratic Institution: Why the Two-sided Market Theories Provide Inadequate Justification for Unrestricted Media Consolidation*, Relazione tenuta al IX Congresso in-

in quanto producono 'effetti indiretti di rete'. Chi compra spazi pubblicitari investe poco nelle aziende appena sorte, perché queste ultime hanno scarse informazioni sui naviganti e quindi sono meno efficaci. Anche gli utenti sono più attratti dal *provider* dominante, in quanto questi, disponendo di più dati e maggiori proventi pubblicitari, ha più risorse per migliorare il servizio. Ciò rende impossibile al nuovo entrante raccogliere dati per finanziare i costi iniziali e avviare le attività[20].

Tali dominanze hanno un impatto sui diritti fondamentali e l'uguaglianza. La dominanza delle piattaforme influisce sulla visibilità dei contenuti, e quindi sulla libertà di espressione. In termini di rispetto del diritto alla *privacy*, la dominanza consente alle piattaforme di imporre le proprie condizioni alla cessione dei dati da parte dell'utente, senza che quest'ultimo possa trovare un trattamento sostanzialmente diverso presso altri *competitor*. Ovvie le ripercussioni sulla partecipazione politica: i grandi attori possono così sorvegliare e indirizzare le condotte degli utenti nascondendo il proprio algoritmo dietro il segreto commerciale.

Alla luce di questa evoluzione, sembra sempre più pertinente l'interpretazione di quella parte della dottrina che legge la *competition law* in senso costituzionalmente orientato: non come corpo di regole distinto, e potenzialmente in contrasto, rispetto ai diritti fondamentali, bensì come strumento delle libertà stesse[21]. La medesima

---

ternazionale della IACL, Oslo, 2014, in *www.jus.uio.no*, pp. 7-9; N. Newman, *Search, Antitrust and the Economics of the Control of User Data*, in *Yale Journal on Regulation*, vol. 31(2), 2014, pp. 411-420.

[20] Autorité de la concurrence, Bundeskartellamt, *Competition Law and Data*, 10/5/2016, in *http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawanddata-final.pdf*, pp. 11-13. A maggior ragione in quanto in questo settore per condurre l'attività sono necessari elevati investimenti iniziali (J. Varhaert, *The Challenges Involved with the Application of Article 102 TFEU to the Market for Search Engines as part of the New Economy and the implications for the Google-case*, Master Thesis in Intellectual Property Rights, 30/8/2013, in *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2340958*, p. 12).

[21] J. Drexl, *Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Posttruth Politics*, *Max Planck Institute for Innovation and Competition Research Paper* No. 16-16, in *https://ssrn.com/abstract=2881191*, pp. 20 ss.; G. De Minico, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, fasc. 1, 2019, p. 104.

connessione appartiene già alla cultura giuridica dell'Unione Europea, in quanto storicamente l'armonizzazione dei mercati è servita anche ad affermare uguali garanzie sui diritti. Oggi, come si vedrà meglio nel paragrafo successivo, la *competition law*, specie nell'ambito digitale, è oggetto di una 'virata geo-economica'[22]: un'interpretazione che si distanzia dalla semplice affermazione della libera circolazione dei beni e diviene servente a obiettivi più generali di sovranità digitale e politica economica.

L'esposizione dei valori in gioco mostra che i dati – inclusi quelli processati nelle telecomunicazioni – hanno caratteristiche che li pongono al centro di un crocevia di interessi. Oltre a essere un *asset* prezioso dell'economia digitale, essi sono diventati un'infrastruttura critica, destinata a impattare sulla sicurezza interna ed esterna dei confini. Tale circostanza è osservabile nel mutamento di segno che la *policy* eurounitaria sta seguendo nel corso degli anni, con conseguenti revisioni delle opzioni di *competition law* adottate dall'UE.

## 3. *Il contesto geopolitico e il nuovo approccio delle* policy *digitali eurounitarie*

Lo scenario sopra individuato, come un 'fermo immagine' di una scena in continuo movimento, descrive a fini illustrativi la situazione esistente allo scorso decennio e le relative questioni, oggi affrontate con un nuovo approccio. È ora il momento, dunque, di approfondire la visuale, guardando a come la disciplina del digitale, qui osservata nel prisma dei *big data*, stia evolvendo insieme ai recenti cambiamenti geopolitici, in cui diverse crisi – da quella climatica a quella bellica – hanno comportato una sostituzione dell'ideologia del libero mercato con un approccio di *partner state* e successivamente di reciproco intreccio tra difesa ed economia. Ad avviso di chi scrive, tali mutamenti dimostrano altresì quello che si è detto sulla *competition law*, che essa – lungi dall'essere una pura disci-

[22] A. Herranz-Surrallés, C. Damro, S. Eckert, *The geoeconomic turn of the single European market? Conceptual challenges and empirical trends*, in *JCMS: Journal of Common Market Studies*, vol. 62(4), 2024, cit. in S. Heidebrecht, *Digital Policy as a Driver of Integration: Spillover Effects and European Commission Empowerment*, in *Politics and Governance*, vol. 13, 2025, p. 2.

plina tecnica – si fa strumento dei più ampi scopi di *governance* dell'UE, assumendosi obiettivi diversi in base ai diversi orientamenti politico-giuridici.

La disciplina del digitale deve essere inquadrata nel più ampio discorso politico eurounitario, dove – negli anni successivi alla crisi del 2008 – si è verificata una transizione dal linguaggio austeritario e tecnocratico a uno progressivamente più attento all'intervento pubblico nell'economia, guidato da priorità politiche comuni. Alla base di tale mutamento si può considerare la coincidenza di diversi fattori, quali la crescita del malcontento per i tagli alla spesa, che impedivano altresì alcuni investimenti strategici degli Stati, ma anche la necessità di rispondere alla crisi post-pandemica successiva al 2020. Una direzione parzialmente nuova è inaugurata nel *Next Generation European Union*, che realizza un intervento dello Stato nell'economia, assistito da fondi presi in prestito dall'Unione sul mercato, da spendere in base a strumenti regolativi condizionali appositamente predisposti; di conseguenza, si è sperimentata in modo massivo l'incentivazione pubblica diretta come nuova modalità per favorire l'innovazione, anche rispetto al settore digitale. Tale sperimentazione ha assunto accenti sempre più chiaramente connessi all'affermazione della sovranità esterna quando – in seguito alla degenerazione della guerra in Ucraina – le *policy* eurounitarie hanno spinto perché gli Stati prendessero decisioni comuni di investimento orientate alle spese militari, assistite altresì dalle nuove flessibilità di bilancio inserite a tale scopo[23].

Il mutamento ha finito per impattare sulla *competition law*, su cui sono cresciute le pressioni rispetto alla necessità di integrare al proprio interno considerazioni di protezione esterna. Ad esempio, nel 2019 le posizioni di alcuni Ministeri degli Stati membri hanno

[23] European Commission, *White Paper for European Defence - Readiness 2030*, 3/2025, 16. Cfr. Bruxelles, 22.4.2025. Cfr. anche la *Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO che modifica i regolamenti (UE) 2021/694, (UE) 2021/695, (UE) 2021/697, (UE) 2021/1153, (UE) 2023/1525 e (UE) 2024/795 per quanto riguarda l'incentivazione di investimenti nel settore della difesa nell'ambito del bilancio dell'UE per attuare il piano "ReArm Europe"*, COM(2025) 188 final, 2025/0103(COD). Cfr. A. Guazzarotti, *Fluidità del soggetto neoliberale e integrazione europea ai tempi del "Rearm Europe"*, in *Costituzionalismo.it*, fasc. 1, 2025, pp. 86-87.

affermato che la politica delle fusioni non tenesse abbastanza in conto le specificità delle aziende controllate da Stati terzi[24].

Rispetto al digitale, sempre più aspetti della *policy* UE sembrano essere ascrivibili all'idea della *digital sovereignty*, intesa come «la capacità di uno Stato di governare, regolamentare e proteggere in modo indipendente le proprie infrastrutture digitali, i flussi di dati e le attività online, senza indebite influenze o interferenze esterne»[25]. Quest'ultima è stata propugnata da diversi Paesi in modalità differenti, con maggiore enfasi sul controllo governativo della tecnologia o della sua sottoposizione a una disciplina riguardante i diritti della persona[26]. Nel caso dell'Unione, la sovranità tecnologica è stata posta al centro di un insieme di *policy*[27], laddove essa è intesa come «capacità dell'Europa di agire in modo indipendente nel mondo digitale e dovrebbe essere intesa sia in termini di meccanismi di protezione che di strumenti offensivi per promuovere l'innovazione digitale (anche in collaborazione con aziende non UE)»[28]. Un ulteriore passo avanti, sotto la seconda Commissione Von der Leyen, ha visto la creazione di una figura di Vicepresidente esecutiva per la Sovranità tecnologica, la sicurezza e la democrazia, incaricata di garantire la *leadership* globale, la sicurezza e la resilienza dell'UE[29].

---

[24] Bundesministerium fur Wirtschaft und Energie - Ministère de l'économie et des finances - Ministerstwo Przedsiębiorczości i Technologii, *Modernising EU Competition Policy*, 2019, p. 1.

[25] J. Pohle, T. Thiel, *Digital sovereignty*, in *Internet Policy Review*, vol. 9(4), 2020, p. 8.

[26] Per uno sguardo comparato: In Search of Digital Sovereignty and Strategic Autonomy: D. Broeders, F. Cristiano, M. Kaminska, *Normative Power Europe to the Test of Its Geopolitical Ambitions*, in *Journal of Common Market Studies*, vol. 61(5), 2023, pp. 163 ss. Ad avviso di Chander e Sun, fanno parzialmente eccezione gli Stati Uniti, che per qualche tempo hanno ostacolato, più che difeso, l'idea della sovranità digitale, per via della loro posizione di potere commerciale: A. Chander, H. Sun, *Introduction. Sovereignty 2.0*, in Id. (a cura di), *Data Sovereignty. From the Digital Silk Road to the Return of the State*, Oxford University Press, Oxford, 2023 (si vedano, con una più ampia panoramica comparata, le pp. 8 ss.).

[27] H. Carrapico, B. Farrand, *EU Data Sovereignty: An Autonomy-Interdependence Governance Gap?*, in *Politics and Governance*, vol. 13, 2025, pp. 2-3.

[28] T. Madiega, *Digital sovereignty for Europe*, EPRS | European Parliamentary Research Service, EPRS Ideas Paper Towards a more resilient EU, 2020, p. 1.

[29] U. von der Leyen, *Mission letter to Henna Virkkunen, Executive Vice President designate for tech sovereignty, security and democracy*, 2024, in *https://commis-*

La destabilizzazione geopolitica prodotta attraverso il digitale è emersa nettamente con la minaccia della disinformazione e della profilazione delle persone votanti, allorché è stata chiara l'interferenza delle piattaforme – e di potenziali attori esterni attraverso le stesse – rispetto ai momenti più delicati della politica nazionale, vale a dire le elezioni[30]. Infatti, lo *Special Report on European Media Sovereignty* ha messo in evidenza la sfida rappresentata dalla presenza di attori globali che non rispettano le regole e i valori fondamentali dell'Unione e mettono l'appropriazione e monetizzazione dei dati al centro della propria strategia[31]. Successivamente, la pandemia ha dato ulteriore rilevanza al tema, e non solo in termini economici. Infatti, la digitalizzazione della maggior parte delle attività quotidiane ha confermato il ruolo cruciale delle tecnologie, inducendo il Consiglio Europeo a introdurre nella sua *roadmap* per la ripresa un invito ad agire per l'autonomia strategica dell'Unione Europea, in particolare rispetto alle capacità, infrastrutture e tecnologie digitali[32]. Infine, il c.d. Rapporto Draghi lega in modo ancora più stretto la geopolitica e l'economia digitale, affermando che «L'intensificarsi della concorrenza geopolitica e le politiche industriali aggressive dei paesi terzi in materia di esportazioni ad alto contenuto tecnologico stanno riducendo la sicurezza delle importazioni dell'UE di tecnologie critiche (ad esempio semiconduttori) e fattori produttivi (ad esempio materie prime critiche). È essenziale ripristinare la sicurezza delle catene di approvvigionamento per le tecnologie critiche rafforzando le capacità e le risorse dell'UE lungo l'intera catena del valore in termini di prodotti finali e piattaforme di servizi»[33].

---

*sion.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en-filename=Mission%20letter%20-%20VIRKKUNEN.pdf*, p. 6.

[30] C. Gérard, *10. Les données numériques au coeur de nouveaux conflits géopolitiques*, in *Regards croisés sur l'économie*, n. 2(23), 2018, p. 139.

[31] G. Klossa, *Towards European Media Sovereignty. An Industrial Media Strategy to leverage Data, Algorithms and Artificial Intelligence*, report Commissioned by the European Commission, 2019, p. 11.

[32] European Council, *A ROADMAP FOR RECOVERY Towards a more resilient, sustainable and fair Europe*, 2020, p. 4.

[33] M. Draghi, *The future of European competitiveness. Part B | In-depth analysis and recommendations*, 2024, p. 67.

Ulteriore dimostrazione di tale tensione nelle *policy* sul digitale è la regolazione eurounitaria della *cybersecurity*, che è nata con l'obiettivo di normare il mercato unico, ma ha visto successivamente l'ingresso di preoccupazioni di diversa natura: l'ingresso della disinformazione nel panorama delle minacce (2016-2019) e successivamente il Covid-19 e Guerra in Ucraina. Se la prima ha minacciato la tenuta delle democrazie europee all'epoca del digitale – come è apparso in modo eclatante con l'annullamento delle elezioni in Romania nel 2024 – le seconde prendono atto di un ambiente internazionale più ostile e segnano un più deciso superamento dell'ortodossia del libero mercato a favore di una ridefinizione dei principi fondamentali della globalizzazione guidata dal mercato, volta a riportare la produzione in Europa e così affermare la sovranità digitale.

Il settore delle telecomunicazioni ha risentito di tali mutamenti, in quanto coinvolto in diverse decisioni destinate a tutelare la sicurezza nazionale. Si pensi, ad esempio, agli accordi stipulati da alcuni Stati membri per il *contact tracing* durante il Covid, con l'obiettivo di supportare la prevenzione del virus. Oppure, si può considerare la minaccia percepita da alcune autorità all'interno dell'Unione rispetto all'ingresso sul mercato di Huawei per il 5G[34]. Dal punto di vista regolativo, almeno due documenti sembrano preludere a un cambiamento regolativo dell'Unione Europea. Il primo è il Rapporto Draghi che – nell'ottica dell'autonomia tecnologica sopra chiarita – evoca il regime asimmetrico come causa di un'eccessiva frammentazione del settore, che beneficia le persone consumatrici, ma mina la competitività dell'Unione Europea. Il secondo è l'iniziativa della Commissione che – citando esplicitamente la minaccia russa – invita a riprendere i lavori verso un aggiornamento della *Data Retention*, a completamento delle altre iniziative che mirano alla difesa verso l'estero[35].

---

[34] Redazione ANSA, *Breton, 'Huawei e Zte sono una minaccia, escluderle da 5G'*, in *ANSA.it*, in *https://www.ansa.it/europa/notizie/rubriche/altrenews/2023/06/15/breton-huawei-e-zte-sono-una-minaccia-escluderle-da-5g_57f2295b-2dc5-4330-96cb-36c1aa6051c.d.html*.

[35] *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on ProtectEU: a Euro-*

La disciplina dei *big data* ha avuto una simile evoluzione, con il progressivo abbandono della *deregulation* favorevole ai colossi *data driven*. In questo senso, diverse scelte dell'Unione sono state interpretate come un tentativo di affermare la propria *data sovereignty*, la possibilità di controllare i dati per interessi ritenuti strategici a livello eurounitario e di evitare che essi siano impiegati per apportare minacce esterne al territorio[36].

Un primo passo in tal senso è individuabile nella *European Data Strategy*[37], che propone un cambio di approccio basato sulla condivisione di dati come motore di sviluppo dell'impresa europea, in competizione con altre economie su scala globale. In tal senso, l'innovazione è perseguita con la condivisione dei dati in luogo della gara alla loro appropriazione esclusiva, in quanto si ritiene che la prima sia necessaria a superare la frammentazione dell'industria europea, accrescere la competitività e raggiungere l'autonomia da Paesi stranieri. Da questa strategia hanno origine un insieme di norme che stanno cambiando il volto della disciplina sui dati. Il *Data Act*[38] prevede l'accesso dell'utente ai dati del prodotto (artt. 3-4) e la loro portabilità, con la possibilità di condividere i dati con terze parti nel caso in cui si voglia cambiare fornitrice (artt. 5-6)[39].

---

*pean Internal Security Strategy*, COM(2025) 148 final, Strasbourg, 1.4.2025. Sulla base di tale comunicazione, la Commissione Europea ha aperto un *Impact assessment on retention of data by service providers for criminal proceedings*, per riflettere su una nuova normativa.

[36] M. Lukings, A.H. Lashkari, *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance An Overview from a Legal Perspective*, Springer, Cham, 2022, pp. 24 ss. X. Gao, X. Chen, *Geopolitics and Transnational Data Governance*, in *Politics and Governance*, vol. 13, 2025, p. 2; F. Cristiano, L. Monsees, *Beyond the Ban: TikTok and the Politics of Digital Sovereignty in the EU and US*, in *Politics and Governance*, vol. 13, 2025, pp. 4-5.

[37] *Comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni Una strategia europea per i dati*, COM(2020) 66 final, Bruxelles, 19.2.2020.

[38] *Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance)*, PE/49/2023/REV/1, OJ L, 2023/2854, 22.12.2023.

[39] Peraltro, ci si è domandato se la nozione di *data sovereignty* adottata dall'UE non sia connotata da accenti protezionistici di natura commerciale: S. Torregiani, *Il Data Act: una versione europea del Data Nationalism?*, in *Rivista italiana di informatica e diritto*, n. 2, 2023, pp. 139-140.

Sono previste altresì alcune condizioni che disciplinano la cessione dei dati medesimi, quali: l'obbligo per il *provider* di mettere a disposizione i dati a condizioni eque, ragionevoli e non discriminatori (c.d. FRAND) e in modo trasparente al nuovo *provider* (art. 8); la previsione di un compenso ragionevole e non discriminatorio per la messa a disposizione dei dati (art. 9); la disciplina di clausole abusive tra imprese (art. 13). D'altra parte, il *Data Governance Act*[40] mira a rafforzare la condivisione dei dati, creando un *framework* idoneo ad assicurare fiducia all'interno del sistema di condivisione.

Per trarre un bilancio, si può osservare che la *competition law* in rete e la disciplina del digitale in genere sono state influenzate da preoccupazioni che esulano dallo stretto calcolo economico, per attingere a un ambito più prossimo alla sicurezza, interna ed esterna. Alla luce di tale rilievo, ci si domanda di seguito come tale approccio possa essere completato alla luce di una comprensione più ampia di sovranità digitale, intrinsecamente connessa ai diritti democratici e di autodeterminazione.

## 4. Digital sovereignty *e Autodeterminazione Informativa*

La politica sui dati appena descritta sembra esprimere un mutamento di indirizzo: dalla concorrenza come tutela dell'appropriazione dei dati alla concorrenza come condivisione delle informazioni medesime. Si rilevava sopra che la più recente normativa cerca di arricchire l'obiettivo della concorrenza, interpretato come servente la sovranità digitale e la sicurezza interna ed esterna dell'Unione, non si può dire rispetto a un altro dei valori menzionati nel paragrafo 2. Resta da vedere se e fino a che punto tale mutamento sia rispettoso dei valori legati all'autodeterminazione informativa o abbia arricchito la normativa al solo scopo di difesa.

In merito, si devono notare alcune aperture, ma anche diversi limiti, di quella parte della disciplina destinata ad ampliare l'auto-

[40] *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)*, PE/85/2021/REV/1, OJ L 152, 3.6.2022 d'ora in poi, DGA.

determinazione informativa. Infatti, il *Data Act*, in primo luogo, non disciplina alcuna forma di apertura generalizzata dei dati per l'interesse generale[41], bensì solo quella che avviene con il consenso dell'utente e per il suo vantaggio commerciale (consid. 35); tale scelta continua a costituire un ostacolo rispetto alla piena appropriazione dei dati da parte delle persone cittadine, abitanti e *prosumer*. D'altra parte, il *Data Governance Act* prevede la possibilità trasferimento coattivo di dati dalle imprese al soggetto pubblico, realizzando così la prevalenza del bene collettivo; tuttavia, tale facoltà è condizionata alla ricorrenza di casi specifici di eccezionale necessità legati all'interesse pubblico[42] (art. 14).

Infine, si prevedono altresì alcuni dispositivi più avanzati, rimessi tuttavia all'adesione volontaria delle entità regolate: in questo senso va la disciplina dei *data intermediaries* (art. 2, n. 11; art. 10) e il *data altruism* (consid. 46, capo IV).

I *data intermediaries* sono definiti come «servizi[o] che mira[no] a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali» (art. 2). L'ordinamento vuole che tali soggetti siano terzi rispetto al trattamento

---

[41] Questa può essere vista come una prospettiva futura della regolazione: E. Cremona, *Quando i dati diventano beni comuni: modelli di* data sharing *e prospettive di riuso*, in *Rivista italiana di informatica e diritto*, n. 2, 2023, pp. 125-126.

[42] J. Chu, *Chapter V of the Data Act - Which should be the legal basis for B2G data sharing: 'exceptional need' or 'public interest'?*, in C. Ducuing, T. Margoni, L. Schirru (a cura di), *op. cit.*, pp. 50-52. Cfr. Commission Staff, *Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)*, Commission Staff Working Document, SWD/2020/295 final; European Parliamentary Research Service, *Governing data and artificial intelligence for all: Models for sustainable and just data governance*, 2022, in *https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf*; Commission - Directorate General for Communications Networks, *Content and Technology, Towards a European strategy on business-togovernment data sharing for the public interest: final report prepared by the High-Level Expert Group on Business-toGovernment Data Sharing'*, 2021, in *https://op.europa.eu/en/publication-detail/-/publication/d96edc29-70fd-11eb-9ac9-01aa75ed71a1*.

dei dati, con l'esclusione della possibilità per tali soggetti di processare e valorizzare essi stessi i dati, invece che fungere da intermediari in un rapporto tra i titolari dei dati e utenti (art. 2). A tal fine, sono previste delle regole comportamentali, ma anche di separazione strutturale (art. 12). Sono altresì esclusi i servizi utilizzati da un titolare dei dati per consentire l'utilizzo dei propri dati e i servizi di condivisione dei dati di natura non commerciale offerti da enti pubblici (art. 2). Viceversa, i servizi di intermediazione dei dati possono offrire servizi specifici strumentali all'intermediazione stessa, «come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi» (art. 12).

Tali soluzioni hanno il vantaggio del pragmatismo: a oggi, diverse iniziative di condivisione di dati (*data sharing initiatives – DSI*) si configurano giuridicamente come *data intermediaries*. Di conseguenza, l'istituto, così costruito, si presta ai fini della *data sovereignty* nella misura in cui può servire a creare 'corpi intermedi' – sul modello delle organizzazioni sindacali – capaci di mediare negoziazioni collettive che coinvolgono anche i diritti fondamentali. Una simile entità sembra poter prendere la forma delle cooperative di dati (consid. 31, art. 10, lett. *c*), DGA)[43]. Queste ultime sono descritte in modo generale dal diritto eurounitario[44], con flessibilità anche nella loro forma giuridica, fermo restando lo scopo di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati. La norma non prevede esplicitamente che l'intermediazione possa avere una natura economica solidale, ma neanche impone che si tratti di un ente a scopo di lucro; pertanto, sarebbe ben possibile costituire un organismo di natura cooperativa capace di tenere in considerazione non soltanto gli interessi economici di chi produce, ma

[43] Sui diversi tipi di *data intermediaries*: D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law and Technologies*, n. 1, 2022, pp. 49-51.

[44] F. BRAVO, *Le Cooperative di Dati*, Project Papers del progetto di terza missione Cooperative di Dati dell'Alma mater studiorum di Bologna, in *https://site.unibo.it/cooperative-di-dati/it/attivita-di-ricerca/pubblicazioni/bravo_le_cooperative_di_dati.pdf*, pp. 4 ss.

anche i diritti fondamentali delle diverse soggettività coinvolte. Peraltro, la norma sembra già essere costruita presupponendo che esista un'iniquità di relazione rispetto al *provider* che utilizza i dati, in quanto si estende anche alla cooperativa di dati l'impossibilità di fornire servizi ai propri soci, nettamente derogatoria rispetto all'idealtipo della cooperativa. Tale regola, ancorché possa apparire eccessivamente rigida[45], sembra ragionevole se si considerano i concreti squilibri di potere tra chi produce e chi processa i dati, che rendono difficilmente pensabile una cooperazione e fanno pensare, piuttosto, che sia necessaria un'aggregazione di interessi collettiva di chi conferisce i dati, indipendente dai *provider* stessi, perché la cooperativa possa tutelare efficacemente gli interessi dei soci.

Infine, alcune proposte *de iure condendo* potrebbero enfatizzare l'utilità dello strumento per riequilibrare situazioni di svantaggio.

Da un punto di vista sostanziale, è necessario che il soggetto pubblico determini a livello eurounitario i principi d'uso dei dati, con un quadro etico e normativo capace di tenere conto delle situazioni di potere e delle conseguenti necessità ridistributive[46].

In secondo luogo, l'efficacia delle previsioni si arresta allorché il *data intermediary* deve arrestarsi di fronte al mancato consenso della persona titolare dei dati, anche quando vi dovesse essere una chiara prevalenza dell'interesse generale. La previsione di uno statuto specifico per le cooperative di dati potrebbe in futuro dare luogo a vere e proprie deleghe a una negoziazione collettiva da parte di specifiche categorie di *data intermediaries*[47], sul modello

---

[45] *Ibidem*, p. 17.

[46] In questo senso: European Law Institute - American Law Institute, *Principles for a data economy: data transactions and data rights*, 2018, in *https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/data-economy/*. Cfr. L. Petrone, *Il mercato digitale europeo e le cooperative di dati* Project Papers del progetto di terza missione Cooperative di Dati dell'Alma mater studiorum di Bologna, in *https://site.unibo.it/cooperative-di-dati/it/attivita-di-ricerca/pubblicazioni/bravo_le_cooperative_di_dati.pdf*, pp. 6-7.

[47] L. Petrone, *op. cit.*, pp. 14-15. In tema di *data altruism*, ma – ad avviso di chi scrive – nella medesima logica: W. Veil, *Data altruism: how the EU is screwing up a good idea*, AlgorithmWatch discussion paper, in *https://algorithmwatch.org/en/eu-and-data-donations/*, pp. 4-5.

delle organizzazioni sindacali, in vista dell'apertura dei dati. In tal caso, dovrebbero essere previste misure vincolanti sulla 'porta aperta', sulla parità di trattamento delle persone socie, sul voto capitario, non determinato dall'investimento economico, sui diritti partecipativi a favore di produttori e produttrici, sullo *standing* dei soggetti diversi titolati a intervenire – ad esempio, consumatori e consumatrici, cittadini e cittadine, etc. – come esponenti dell'interesse generale.

Naturalmente, a tal fine si richiedono investimenti volti ad appianare il *gap* delle competenze *digital*. Si rende dunque necessario un intervento pubblico per l'alfabetizzazione digitale, soprattutto delle categorie più precarie, volta alla dotazione di strumenti per l'analisi critica delle informazioni e l'autodeterminazione effettiva nelle scelte sui dati.

Normalmente, le imprese *high tech* operano una vera e propria 'curatela' sui dati, intesa come pratica di selezionare, rappresentare e conservare i contenuti, anche in base a valutazioni contingenti e prospettive future. La medesima 'curatela' dovrebbe poter essere esercitata dalla comunità, che potrebbe sviluppare proprie tecnologie per scopi di interesse generale. Tuttavia, 'free access isn't necessarily fair access', laddove non sia equamente ridistribuita la capacità e la possibilità giuridica di farsi protagonista, invece che semplice 'pubblico' di tale curatela. Fuor di metafora, serve una democratizzazione delle competenze per consentire a soggetti individuali e collettivi di fare scelte informate dai dati, sulla base delle proprie opzioni valoriali.

## 5. *Conclusioni*

L'analisi ha mostrato come la regolazione dei *big data* nelle telecomunicazioni sia ormai alle porte di un profondo cambiamento che realizza un intreccio sempre più stretto tra antitrust, geopolitica e diritti fondamentali. Il campo, che fino a poco tempo fa era dominato da una certa ideologia del libero mercato – che vedeva l'innovazione alimentata dall'accaparramento di dati – sta progressivamente aprendo la strada a un regolatore più attento alla sovranità digitale, alla sicurezza e alla difesa collettiva.

Nel nuovo scenario descritto, i *big data* e le telecomunicazioni sono un'infrastruttura critica sulla quale si gioca l'autonomia strategica dell'Unione, in un momento in cui sembra essere in gioco la sicurezza e la solidità democratica dei suoi Stati membri. La guerra, le interferenze elettorali, la pandemia, la competizione tecnologica con attori fuori dall'Europa hanno mostrato come la regolazione del digitale non sia più dissociabile da una dimensione geopolitica. Conseguentemente, la *competition law* ha subito una rilevante 'svolta geo-economica', trasformandosi sempre più in strumento di politica industriale e difesa dei valori dell'UE.

È una transizione ben simboleggiata dalla nuova regolazione – in particolare dal *Data Governance Act* e il *Data Act* – che promuove la condivisione dei dati come alternativa all'accaparramento, a beneficio della resilienza e della competitività del mercato unico. Tuttavia, questo nuovo paradigma non è privo di ambiguità. Da una parte, infatti, la normativa mira a contrastare le asimmetrie di potere delle grandi piattaforme, ridurre le dipendenze strategiche, nonché demercificare il dato a favore di una rilevanza più spiccatamente sociale. Dall'altra parte, però, rischia di non arrivare fino in fondo in questa opera, in quanto non ha come obiettivo primario un vero riequilibrio di potere a favore delle persone.

L'impegno che si apre per il contesto europeo è pertanto duplice. Da una parte, bisogna costruire una sovranità digitale che sia anche democratica, in cui il controllo sui dati sia esercitato collettivamente, eventualmente attraverso soggetti come i *data intermediaries* e le *data cooperative*. Dall'altra, è necessario ridurre il divario di competenze e favorire un'alfabetizzazione digitale, in modo che cittadini, lavoratori e comunità siano protagonisti – e non solo vittime – dell'avvento digitale.

In prospettiva, il futuro della regolazione dei *big data* non potrà prescindere da una presa di posizione decisa rispetto all'idea democratica che l'UE vuole mettere al centro della propria sovranità digitale. Solo a queste condizioni quest'ultima cesserà di essere una semplice reazione difensiva alle minacce esterne, per diventare un progetto positivo di liberazione civile.

CHIARA GALBERSANINI

# LA TUTELA DEI DATI PERSONALI DI NATURA CULTURALE NELLO SPAZIO DIGITALE: CRITICITÀ E SFIDE EMERGENTI



## 1. *Introduzione*

I dati *personali* di carattere *culturale* hanno assunto una rilevanza specifica nello spazio digitale[1]: se è vero, infatti, che la nozione

[1] Per un approfondimento in senso ampio sul tema della *governance* europea della società digitale digitale, cfr. S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, F. PIZZETTI, *La regolazione europea della società digitale*, Giappichelli, Torino, 2025; M. OROFINO, *Trattamento dei dati personali e libertà di espressione e di informazione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Editoriale Scientifica, Napoli, 2017; G. DE MINICO, *Libertà in Rete. Libertà dalla Rete*, Giappichelli, Torino, 2020; L. BOLOGNINI, E. PELINI, M. SCIALDONE, *Digital Services Act e Digital Markets Act. Definizioni e prime applicazioni dei nuovi regolamenti europei*, Giuffrè, Milano, 2023; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016; L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in L. SCAFFARDI (a cura di), *I "profili" del diritto Regole, rischi*

di dato personale di carattere culturale presenta un'elevata complessità concettuale in ragione dell'indeterminatezza insita nel concetto stesso di *cultura*[2] – e non trovi, ad oggi, una definizione espressa nel Regolamento (UE) 2016/679 –, tuttavia taluni dati personali idonei a rivelare l'appartenenza culturale, linguistica o etnica dell'interessato assumono una rilevanza peculiare nello spazio digitale.

Tale aspetto emerge, in particolare, con riferimento ai trattamenti automatizzati di profilazione che si fondano su dati personali di natura culturale e intreccia, da un lato, il profilo della tutela dei dati personali e dell'identità digitale dell'interessato, e, dall'altro, quello della valorizzazione del pluralismo delle espressioni culturali e identitarie a cui l'interessato è esposto nell'ambiente online.

Invero, in primo luogo, l'esperienza di fruizione di determinati contenuti di carattere culturale online si collega in modo diretto al trattamento dei dati personali e, conseguentemente, alla loro tutela nell'ambito del diritto alla protezione dei dati: attraverso processi automatizzati di profilazione[3], l'analisi e l'incrocio di informazioni

---

*e opportunità nell'era digitale*, DPCE - Dossier VII, Giappichelli, Torino, 2018; M. D'Amico, *Costituzione, diritti, algoritmi. Le sfide future per non perdere la bussola del costituzionalismo*, in F. Balaguer Callejòn (coord.), *La Constituciòn del Algoritmo. Recensiones, presentaciones y entrevistas*, Fundaciòn Manuel Giménez Abad, Zaragoza, 2025, p. 157 ss.; P. Perri, *Sorveglianza elettronica, diritti fondamentali ed evoluzione tecnologica*, in collana *Informatica Giuridica*, Giuffrè, Milano, 2020.

[2] Il concetto di cultura costituisce il principale oggetto di studio delle scienze antropologiche: esisterebbero più di centocinquanta definizioni del concetto di cultura. Cfr., *ex multis*, Aa.Vv., *Il concetto di cultura. I fondamenti teorici della scienza antropologica*, Einaudi, Torino, 1970, p. 43 e ss.

[3] Per processo automatizzato di profilazione si intende, ai sensi dell'art. 4 par. 4 del GDPR, «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica». Per un approfondimento sul tema della profilazione algoritmica e delle conseguenze sul piano giuridico, cfr. *ex multis*, G. Sartor, F. Lagioia, *Le decisioni algoritmiche tra etica e diritto*, in U. Ruffolo (a cura di), I*ntelligenza artificiale: il diritto, i diritti, l'etica*, Giuffrè, Milano, 2020; A. Savin, *The EU digital Services Act: Towards a more responsible internet*, in *Copenhagen Business School Law Research Paper*, 21-04-2021; P. Perri, *Obblighi di informazione e sistemi decisionali e di monitoraggio automatizzati (art. 1-bis "Decreto Trasparenza"): quali forme di controllo per i poteri datoriali algoritmici?*, in *Labor*, vol. 1, 2023.

di carattere *culturale* – quali preferenze linguistiche, musicali, editoriali o altri dati personali di natura culturale che evidenziano una *appartenenza* culturale –, è possibile costruire profili altamente dettagliati dell'interessato, che si legano, in particolare, con la dimensione *culturale* dell'*identità personale* di quest'ultimo e con la sua *rappresentazione* nello spazio digitale.

Non solo: si sottolinea che, in alcuni casi, i dati personali di natura culturale – pur non rientrando formalmente nelle "categorie particolari di dati" di cui all'art. 9 del GDPR[4], – risultano, per certi versi, "contigui" ai dati cosiddetti "sensibili", poiché possono essere utilizzati per inferire indirettamente informazioni non fornite dall'interessato, ma che è possibile desumere, ad esempio, dalla loro combinazione: tali informazioni, una volta inferite, possono fornire elementi circa l'appartenenza linguistica, l'origine etnica, le convinzioni religiose e filosofiche.

Mentre, tuttavia, per i cosiddetti dati personali sensibili – qualificati dal GDPR come *categorie particolari di dati personali* ai sensi dell'art. 9 – è prevista una tutela specifica e rafforzata, fondata su un regime di trattamento eccezionale e su rigorosi presupposti di liceità del trattamento – e per i quali l'utilizzo finalizzato a processi automatizzati di profilazione è, in via di principio, vietato –, per i *dati personali di natura culturale* non esiste, allo stato attuale, una disciplina specifica prevista dal GDPR.

E tuttavia, tali dati, pur non essendo formalmente ricompresi tra le categorie speciali di cui all'art. 9 del riferito Regolamento, possono comunque, in taluni casi, rivelare informazioni idonee a esporre l'interessato a rischi di discriminazione[5] o stigmatizzazione linguistico-culturale o a sfondo razziale[6], in particolare quando il

[4] 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 (regolamento generale sulla protezione dei dati).

[5] M. D'Amico, C. Siccardi, *La Costituzione non odia. Conoscere, prevenire e contrastare l'hate speech on line*, Giappichelli, Torino, 2021; M. D'Amico, C. Nardocci, *Intelligenza artificiale e discriminazione di genere: rischi e possibili soluzioni*, in G. Cerrina Feroni, C. Fontana, E. C. Raffiotta (a cura di), *AI Anthology. Profili giuridici, economici e sociali dell'intelligenza artificiale*, Il Mulino, Bologna, 2022, p. 251 ss.

[6] Sul tema, in senso, ampio, cfr. O. Pollicino, P. Dunn, *Intelligenza artificiale e*

loro trattamento può consentire l'inferenza di elementi indicativi dell'*appartenenza linguistico-culturale* dell'interessato.

In secondo luogo, va rilevato come il trattamento di dati personali di natura culturale mediante processi automatizzati di profilazione conduca frequentemente alla formazione di *echo chamber* "monoculturali": tali ambienti digitali, costruiti sulla base delle preferenze culturali dell'interessato e caratterizzati da una marcata omogeneità identitaria, tendono a ridurre sensibilmente la dimensione di tutela e di valorizzazione del pluralismo e della diversità delle espressioni culturali nello spazio online[7].

Scopo del presente contributo sarà, allora, quello di evidenziare, innanzitutto, la *complessità* che la nozione di *dato personale di carattere culturale* implica nello spazio digitale, in assenza, peraltro, di una *definizione giuridica* di "dato culturale" nel quadro del GDPR; di approfondire il rapporto tra trattamento dei dati personali di natura culturale e rischi derivanti dalle pratiche di profilazione automatizzata dell'interessato, con specifico riguardo alla tutela dell'identità personale nello spazio digitale e alla prevenzione di fenomeni discriminatori riconducibili all'appartenenza culturale o linguistica, prendendo in esame, in particolare, il caso della discriminazione linguistico-culturale nell'ambito della selezione del personale.

---

*democrazia*: opportunità e rischi di disinformazione e discriminazione, Bocconi University Press, 2024; C. Nardocci, *Algoritmi, eguaglianza, discriminazione*, Giappichelli, Torino, 2025; G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?*, in *Rivista AIC*, n. 3, 2025; M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI Act*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea dell'intelligenza artificiale nella società digitale*, Giappichelli, Torino, 2025; L.B. Solum, *Artificially Intelligent Law*, in *BioLaw Journal*, n. 1, 2019, p. 57; A. D'Aloia, *Intelligenza artificiale, società algoritmica, dimensione giuridica. Lavori in corso*, in *Quad. Cost.*, n. 3, 2022; M. Orofino, G. Cavaggion, *Lingua e Costituzione: l'irrompere dei linguaggi algoritmici*, in *Rivista AIC*, n. 4, 2023; M. Orofino, F.G. Pizzetti, *Privacy, Minori e cyberbullismo*, Giappichelli, Torino, 2018; A. Simoncini, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal*, n. 1, 2019; A. Simoncini, S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, n. 2, 2019, p. 93.

[7] P. Perri, *L'utilizzo di sistemi d'intelligenza artificiale e di strumenti automatizzati per il contrasto alle espressioni d'odio nella prospettiva della protezione dei dati personali*, in S.V. Parini (a cura di), *Parole pericolose: conflitto e bilanciamento tra libertà e limiti: una prospettiva trasversale*, Giappichelli, Torino, 2023.

Verranno successivamente esaminate le disposizioni del GDPR che disciplinano i trattamenti automatizzati, inclusa la profilazione, con l'obiettivo di evidenziare come tali norme mirino, se non ad eliminare, quantomeno a mitigare i rischi di pratiche discriminatorie, anche linguistico-culturali. In parallelo, verrà altresì richiamato, per la sua pertinenza al tema, il quadro regolatorio delineato dal *Digital Services Act* (DSA) e dall'*AI Act*, con riferimento alla tutela del principio di non discriminazione su base linguistico-culturale.

Ci si interrogherà, infine, sulla necessità o meno di prevedere una tutela "rafforzata" dei dati personali di natura culturale, anche alla luce, da una parte, delle più recenti evoluzioni del diritto europeo in materia di *data governance*, dove anche la dimensione culturale e linguistica dei dati assume un rilievo crescente, e, dall'altra parte, alla diffusione di pratiche discriminatorie fondate su pregiudizi di natura linguistica e culturale nello spazio digitale.

## 2. *La* complessità *della nozione di dato personale di carattere culturale nello spazio digitale*

Non esiste, ad oggi, una definizione giuridica di *dato personale di carattere culturale* all'interno del GDPR, né la categoria di "dati culturali" viene mai nominata nel testo del riferito Regolamento: una definizione giuridica di dato personale di carattere culturale non è nemmeno riscontrabile in altri documenti europei sulla protezione e circolazione di dati di natura culturale[8].

D'altra parte, fornire una definizione univoca di *dato culturale* risulterebbe un'operazione particolarmente complessa: in effetti, la nozione di cultura[9] – e, conseguentemente, quella di dato *culturale* – può essere intesa secondo prospettive differenti e molteplici interpretazioni, anche in ambito giuridico[10].

---

[8] Si fa riferimento, in particolare, al Documento "Commission *Recommendation of 10.11.2021 on a common European data space for cultural heritage*" e al precedente "*Commission Recommendation of 27 October 2011 on the digitisation and online accessibility of cultural material and digital preservation*"

[9] Cfr., *ex multis*, Aa.Vv., *Il concetto di cultura. I fondamenti teorici della scienza antropologica*, cit.

[10] M. Ainis, *Cultura e politica. Il modello costituzion*ale, Cedam, Padova, 1991; Ainis M., Fiorillo A., *L'ordinamento della cultura. Manuale di legislazione dei beni cul-*

Invero, mentre la nozione di *dato personale* risulta compiutamente definita dal Regolamento (UE) 2016/679[11], un'eventuale definizione di *dato personale di carattere culturale* incontrerebbe, con ogni probabilità, l'ostacolo rappresentato dall'intrinseca indeterminatezza della nozione di "cultura"[12]: sebbene il concetto di culturale sia stato analizzato «in un infinito numero di libri ed articoli, esiste ancora una grande incertezza riguardo al suo impiego» e «gli antropologi usano questa nozione in modi fondamentalmente diversi»[13].

Secondo una concezione *ristretta* del concetto di cultura, che tuttavia appare oggi superata, la dimensione culturale verrebbe ricondotta esclusivamente all'ambito delle espressioni artistiche, letterarie o linguistiche, trascurando la sua più ampia valenza identitaria[14]: una simile impostazione non sembra, però, risultare adeguata a cogliere la complessità del fenomeno culturale, tanto in una dimensione *offline* quanto *online*[15].

Secondo una concezione *ampia* della nozione di cultura, quest'ultima comprende, invece, l'insieme delle pratiche, dei valori, delle credenze, dei linguaggi, dei comportamenti e delle forme sim-

---

*turali*, III ed., Giuffrè, Milano, 2015. Cfr., inoltre, G. Famiglietti, *Diritti culturali e diritto della cultura. La voce "cultura" dal campo delle tutele a quello della tutela*, Giappichelli, Torino, 2010.

[11] Ai sensi dell'art. 4 del GDPR, per «dato personale» si intende «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». Si segnala, inoltre, che la recente Proposta di Regolamento COM(2025) 837 final – cosiddetto Digital Omnibus –, qualora approvato in via definitiva, andrebbe a chiarire ulteriormente la nozione di dato personale ai sensi dell'art. 4 GDPR, specificando che un'informazione «is not to be considered personal data for a given entity when it does not have means reasonably likely to be used to identify the natural person to whom the information relates». Cfr., in particolare, art. 3 della proposta di Regolamento.

[12] Aa.Vv., *Il concetto di cultura. I fondamenti teorici della scienza antropologica*, cit.

[13] *Ibidem*, p. 43 ss.

[14] Aa.Vv., *Il concetto di cultura. I fondamenti teorici della scienza antropologica*, cit.

[15] A. Lupo, *La nozione positiva di patrimonio culturale alla prova del diritto globale*, in *Aedon Rivista di arti e diritto online*, n. 2, 2019.

boliche attraverso cui gli individui e i gruppi sociali esprimono e costruiscono la propria identità. In questa prospettiva, la cultura non è più solo un prodotto, né si riduce al sapere "alto" o istituzionalizzato, ma si configura come un processo dinamico, tipico dell'esperienza umana, di caratterizzazione dell'identità dell'individuo e della comunità di riferimento[16].

Una tale concezione in senso ampio del concetto di cultura si accosta anche ad una dimensione *online*, dove l'identità culturale dell'individuo si manifesta attraverso interazioni digitali e l'espressione di preferenze culturali. È in tale contesto che il dato personale di natura culturale diviene oggetto di trattamento e di profilazione.

In effetti, pur in assenza di una definizione espressa di dato culturale, il GDPR evidenzia il nesso tra i dati personali e la dimensione culturale dell'identità dell'interessato. L'art. 4 del riferito Regolamento non solo fornisce una definizione di «dato personale», intendendo una «*qualsiasi informazione* riguardante una persona fisica identificata o identificabile», ma precisa che è «da considerarsi *identificabile* la persona fisica che può essere individuata, direttamente o indirettamente, mediante un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o *uno o più elementi caratteristici della propria identità* fisica, fisiologica, genetica, psichica, economica, *culturale* o sociale» (corsivo dell'Autrice).

La disposizione richiamata dell'art. 4 GDPR appare, allora, particolarmente significativa con riferimento alla tutela dei dati personali di natura culturale, perché, pur non fornendo una definizione di dato culturale, riconosce esplicitamente la dimensione *culturale* dell'identità personale, i cui elementi possono concorrere all'identificazione dell'interessato: in altri termini, l'inclusione della componente "culturale" tra gli elementi caratterizzanti l'identità dell'interessato rivela non soltanto una concezione ampia e multidimensionale dell'identità della persona, che trascende gli aspetti meramente fisici, ma introduce – seppur in modo implicito – un riconoscimento delle esigenze di protezione anche per quei dati che

[16] *Ibidem.* Cfr. inoltre R. Miccù, A.L. Tarasco, *Il patrimonio culturale e le sue immagini. Diritto, gestione e nuove tecnologie*, Napoli, Editoriale Scientifica, 2022.

esprimono una dimensione *culturale* dell'identità personale e che consentono l'identificazione, diretta o indiretta, dell'interessato.

In questo senso, si precisa che l'identificabilità *diretta* si riferisce alla circostanza per cui il dato consente di risalire direttamente all'identità dell'interessato, senza la necessità di ulteriori informazioni. Si pensi, ad esempio, al nome, al codice fiscale, all'immagine del volto o a un numero di identificazione univoco: si tratta di elementi che individuano in modo diretto la persona fisica; l'identificabilità *indiretta*, invece – che riguarda maggiormente il caso dei dati personali di natura culturale –, ricorre quando un'informazione non consente, da sola, di individuare l'interessato, ma può farlo se combinata con altri dati disponibili: ad esempio, dati relativi all'ubicazione, all'appartenenza linguistica o culturale, alle abitudini di consumo o al profilo digitale possono, se associati, permettere di identificare una persona in modo univoco[17].

Ne consegue che dati in apparenza "neutri" – quali quelli di natura culturale o linguistica – possono assumere la qualificazione di dati personali ove, nel contesto specifico del trattamento, risultino idonei a consentire l'identificazione, diretta o indiretta, dell'interessato. In tale circostanza, il relativo trattamento dovrà essere regolato dalla disciplina prevista dal GDPR, che, pur non contemplando una regolamentazione specifica circa i dati personali di natura culturale, ne impone la tutela.

## 3. *L'*assenza *di una definizione di dato personale di natura culturale nel GDPR*

Tenendo presente la disciplina prevista dal GDPR, si può, così, osservare che l'assenza di una definizione normativa di dato personale di carattere culturale lascia emergere una sorta di "zona grigia" nella qualificazione di un dato personale come "culturale": tale qualificazione potrebbe, infatti, dipendere da valutazioni contestuali all'uso che di esso viene fatto nel trattamento.

[17] Il Considerando 26 del GDPR chiarisce che per valutare se una persona è identificabile occorre tener conto di «tutti i mezzi ragionevolmente utilizzabili» dal titolare o da terzi per identificare l'interessato, compresi i costi, il tempo necessario e la tecnologia disponibile.

In tale prospettiva, un dato personale di natura culturale potrebbe riferirsi, ad esempio, alle preferenze culturali dell'individuo, al suo rapporto con beni o prodotti culturali, ovvero all'appartenenza a una determinata comunità culturale. Tali elementi assumono rilievo non solo rispetto alla dimensione identitaria del singolo, ma, in taluni casi, anche rispetto a quella collettiva, contribuendo alla caratterizzazione culturale della comunità di riferimento.

In questo orizzonte, occorre, per altro, precisare che anche qualora i dati personali di natura culturale si riferiscano al rapporto del soggetto con un dato patrimonio culturale, si riscontra, soprattutto a livello europeo – e, ancora prima, a livello internazionale –, una tendenza ad assumere una concezione ampia di "patrimonio culturale", non circoscritto al patrimonio culturale *materiale* o ai beni culturali *in senso stretto*, bensì estesa a una dimensione antropologica, identitaria e sociale del patrimonio culturale stesso, idonea a riflettere la complessità delle espressioni culturali individuali e collettive[18].

In particolare, la *Raccomandazione della Commissione Europea relativa a uno spazio comune europeo di dati per il patrimonio culturale*[19], che mira a raccogliere e digitalizzare i dati relativi ai beni culturali materiali e immateriali, riflette una concezione *ampia* di "bene culturale", che non si limita ai soli beni artistici tradizionali, ma include anche linguaggi, memorie collettive, pratiche e forme espressive, con l'obiettivo di assicurare al patrimonio europeo una più ampia circolazione e valorizzazione.

L'art. 3 della Raccomandazione utilizza, infatti, una categoria piuttosto ampia della nozione di "beni del patrimonio culturale", ricomprendendovi beni del patrimonio culturale *materiale*, quali monumenti, siti archeologici, materiale sonoro e audiovisivo, libri, riviste, giornali, fotografie, oggetti museali, documenti d'archivio;

[18] Sulla distinzione tra patrimonio materiale e immateriale e relative tutele nell'ordinamento giuridico nazionale, cfr. F. Rimoli, *Profili costituzionali della tutela del patrimonio culturale*, in E. Battelli, B. Cortese, A. Gemma, A. Massaro (a cura di), *Patrimonio culturale. Profili giuridici e tecniche di tutela*, RomaTre Press, Roma, 2017, 2.

[19] Raccomandazione (Ue) 2021/1970 della Commissione del 10 novembre 2021 relativa a uno spazio comune europeo di dati per il patrimonio culturale.

beni del patrimonio culturale *immateriale*; beni del patrimonio naturale, quali paesaggi e siti naturali, come definiti all'articolo 2 della Convenzione relativa alla protezione del patrimonio culturale e naturale mondiale[20]; beni del patrimonio nato digitale.

Di più: il par. 2 del medesimo articolo specifica che per "patrimonio culturale immateriale" si intendono le pratiche, rappresentazioni, espressioni, conoscenze, competenze – nonché strumenti, oggetti, artefatti e spazi culturali ad essi associati – che le comunità, i gruppi e, in alcuni casi, gli individui riconoscono come parte del loro patrimonio culturale, ai sensi dell'articolo 2 della Convenzione per la salvaguardia del patrimonio culturale immateriale[21].

Accanto alla Raccomandazione della Commissione Europea 2921/1970, dello stesso tenore anche la Decisione 1194/2011/UE che istituisce un marchio del patrimonio culturale[22] e che considera "siti", ai sensi dell'art. 2 non solo i monumenti, i siti naturali, subacquei, archeologici, industriali o urbani, i paesaggi culturali, i luoghi della memoria, i beni culturali, ma anche il patrimonio immateriale associato ad un luogo, compreso il patrimonio contemporaneo[23].

D'altra parte, già a livello internazionale, come richiamato, la maggior parte degli strumenti normativi e programmatici in materia di tutela dei beni culturali ha progressivamente adottato, negli ultimi vent'anni, un'accezione ampia della nozione di *patrimonio culturale*. Tale concetto non si limita più al patrimonio artistico in senso stretto, ma ricomprende l'insieme delle espressioni identitarie delle comunità, riconoscendo così alla "cultura" un significato anche antropologico e dinamico.

---

[20] Convenzione UNESCO sulla protezione del patrimonio culturale e naturale mondiale, Parigi, 16 novembre 1972.

[21] Convenzione UNESCO per la salvaguardia del patrimonio culturale immateriale 2003, Parigi, 17 ottobre 2003.

[22] Decisione n. 1194/2011/UE del Parlamento europeo e del Consiglio, del 16 novembre 2011, che istituisce un'azione dell'Unione europea per il marchio del patrimonio europeo.

[23] Cfr. Art. 2, Decisione n. 1194/2011/UE: «Ai fini della presente decisione, si intende per: 1) «siti», i monumenti, i siti naturali, subacquei, archeologici, industriali o urbani, i paesaggi culturali, i luoghi della memoria, i beni culturali e il patrimonio immateriale associati a un luogo, compreso il patrimonio contemporaneo».

È stata, in particolare, la *Convenzione UNESCO per la Salvaguardia del patrimonio immateriale dell'umanità* del 2003 ratificata dall'Italia con legge n. 167 del 27 settembre 2007 ad estendere fortemente il "perimetro" del concetto di patrimonio culturale sino a includervi «le prassi, le rappresentazioni, le espressioni, le conoscenze, il *know-how* – come pure gli strumenti, gli oggetti, i manufatti e spazi culturali associati agli stessi – che le comunità, i gruppi e in alcuni casi gli individui riconoscono in quanto parte del loro patrimonio culturale»[24].

In questo quadro, pertanto, sebbene le iniziative europee sulla creazione di *data spaces* culturali risultino lontane dall'elaborazione di una vera e propria definizione di *dato culturale* e, soprattutto, non riguardino strettamente la nozione di dato *personale* di carattere culturale, si può, tuttavia, ipotizzare che una eventuale definizione a livello europeo di dato culturale e, in particolare, di dato *personale* di carattere culturale, qualora introdotta, possa accostarsi, anch'essa, ad un'accezione *ampia* di "cultura", e non solo riferita ai beni culturali materiali, che già caratterizza la tutela e la valorizzazione del patrimonio culturale nello spazio digitale.

In questa prospettiva, appare plausibile considerare che la categoria concettuale di *dato personale di carattere culturale* – non definita, ad oggi, dal GDPR – non si limiti esclusivamente alle informazioni che denotano il rapporto dell'individuo con beni culturali materiali in senso stretto, quali opere e prodotti culturali, ma debba essere estesa anche a quei dati personali che riguardano il rapporto del soggetto con beni immateriali e quindi, plausibilmente, a dati che siano legati anche alla dimensione *identitaria* del soggetto.

Il *dato personale di carattere culturale* potrebbe, così, riflettere l'identità culturale dell'interessato, definita dalla sua cultura di riferimento (lingua, valori, pratiche culturali), evidenziando al contempo il legame tra dato, identità culturale e appartenenza a un gruppo più ampio, quale una minoranza, una comunità nazionale, religiosa o etnica.

In questa prospettiva, si osserva, in aggiunta, che il dato personale di carattere culturale, pur non rientrando, ad oggi, nelle cate-

[24] Cfr. art. 2, comma 1, Convenzione Unesco per la Salvaguardia del patrimonio immateriale dell'umanità del 2003.

gorie particolari di dati enumerate dall'art. 9 del GDPR[25], si pone in una relazione di stretta contiguità con alcune di esse, avvicinandosi, per sua natura, a dati che rivelano le opinioni filosofiche o ideologiche e, in alcuni casi, a dati idonei a rivelare l'origine etnica dell'interessato e la sua appartenenza religiosa.

In effetti, ad esempio, attraverso dati che esprimono una preferenza personale per associazioni culturali legate a movimenti filosofici o a correnti ideologiche, potrebbero essere inferiti quei dati personali che delineano l'orientamento etico dell'interessato. In altri casi, il dato personale di carattere culturale potrebbe indicare l'origine etnica dell'interessato, qualora quest'ultima sia strettamente correlata a particolari appartenenze linguistico-culturali o linguistico-dialettali, a tradizioni, simboli, riti, pratiche culturali caratterizzanti l'appartenenza a determinati gruppi etnici; oppure, ancora, rivelare l'appartenenza religiosa qualora informazioni riguardanti, ad esempio, la partecipazione a pratiche rituali specifiche o l'utilizzo di specifici simboli culturali possano indicare, indirettamente, l'adesione dell'interessato ad una specifica convinzione religiosa.

Occorre, poi, sottolineare che la definizione di *dato personale di carattere culturale* dovrebbe essere elaborata alla luce di quei princìpi fondamentali dell'ordinamento europeo e nazionale che si intrecciano con la tutela del pluralismo culturale, in coerenza con la stessa forma di Stato democratico-pluralista e con i valori dell'Unione europea fondati sul rispetto della diversità culturale e linguistica. Secondo tale prospettiva, nel quadro dell'ordinamento costituzionale nazionale, assumono, in particolare, rilievo l'art. 2 Cost., che tutela il pluralismo in tutte le sue espressioni, anche nella dimensione culturale; l'art. 6 Cost., che impone la protezione delle minoranze linguistiche e delle relative espressioni culturali; e l'art. 9

[25] Il regolamento indica all'art. 9 quei dati rientranti in particolari categorie: si tratta dei dati c.d. "sensibili". Cfr. art. 9 del GDPR, par. 1: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Cost., primo comma, che affida alla Repubblica il compito di promuovere lo sviluppo della cultura, da potersi intendere, quest'ultima, anche in senso antropologico e secondo una visione "plurale" ed "inclusiva", ovvero comprensiva della molteplicità delle tradizioni, dei linguaggi e delle identità culturali presenti nella società contemporanea[26].

In quest'ottica, un ordinamento che si fonda sul principio pluralista – declinato anche nella sua dimensione culturale – dovrebbe adoperarsi quanto più possibile per creare le condizioni necessarie affinché ogni individuo possa pienamente sviluppare la propria identità culturale come singolo, e nel gruppo di appartenenza, tanto in una dimensione *offline* quanto *online*, garantendo al tempo stesso una tutela e una valorizzazione delle diverse lingue e culture minoritarie, non quali «oggetti della memoria», ma, piuttosto, in quanto «patrimoni di sensibilità collettiva vivi e vitali nell'esperienza dei parlanti»[27].

Una definizione di dato culturale dovrebbe, infine, tenere conto, sul piano dell'ordinamento giuridico europeo, dei valori enunciati dall'art. 2 del Trattato sull'Unione europea[28], e in particolare del rispetto del pluralismo come valore fondativo dell'Unione, nonché dell'art. 22 della Carta dei diritti fondamentali dell'Unione europea[29], che impone di rispettare la diversità culturale, religiosa e linguistica.

---

[26] Cfr. M. Ainis, *Cultura e politica. Il modello costituzionale*, Cedam, Padova, 1991, 127; G. Famiglietti, *Diritti culturali e diritto della cultura. La voce "cultura" dal campo delle tutele a quello della tutela*, Giappichelli, Torino, 2010. Sul concetto costituzionale di cultura e sulla sua ambivalenza, si veda T. De Mauro, *Qualche premessa teorica alla nozione di cultura e bene culturale*, in *Il comune democratico*, n. 10, 1978, 16 ss. Sull'etimologia del termine cultura, cfr. in particolare E. Leach, (voce) "*Cultura/culture*", in *Enc. Einaudi*, IV, Torino, 1978, p. 238 ss.

[27] Corte cost., sent. n. 170/2010.

[28] Cfr. Art. 2 TUE: «L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini».

[29] Cfr. Art. 22 Carta dei diritti fondamentali dell'Unione Europea: «L'Unione rispetta la diversità culturale, religiosa e linguistica».

## 4. *Il dato personale di carattere culturale e il suo intreccio con la tutela dell'identità personale dell'interessato e della sua rappresentazione nello spazio digitale*

Assumendo, quindi, la prospettiva secondo cui il *dato personale di carattere culturale* possa essere strettamente connesso alla *dimensione identitaria* dell'interessato, è possibile formulare alcune riflessioni circa il rapporto tra tutela dei dati culturali e protezione dell'identità personale nello spazio digitale.

Il diritto all'identità personale è, infatti, inteso come «l'interesse del soggetto (…) di essere rappresentato, nella vita di relazione, con la sua vera identità, così come questa nella realtà sociale, generale o particolare, è conosciuta»[30], anche sulla base delle sue convinzioni culturali, ideologiche, religiose e delle sue vicende umane e professionali[31].

In particolare, il diritto all'identità personale è stato ricondotto all'«esigenza di "essere se stessi" nella prospettiva di una compiuta rappresentazione della personalità individuale in tutti i suoi aspetti ed implicazioni, nelle sue qualità ed attribuzioni: diritto alla propria identità sottoposta ai medesimi mutamenti della personalità individuale»[32].

È stata la Corte di Cassazione ad affermare che «mentre i segni distintivi (nome, pseudonimo, ecc.) identificano, nell'attuale ordinamento, il soggetto sul piano dell'esistenza materiale e della condi-

---

[30] Cassazione civile, sent. n. 3769 del 22 giugno 1985 in *Foro it*., 1985, I, 2211 ss. Cfr., *ex multis*, in dottrina, A. Cerri, (voce) *Identità personale*, cit., 1; L. Trucco, *Introduzione allo studio dell'identità individuale*, cit., 245 ss. e 263 ss.; G. Pino, *La tutela dell'identità personale*, Bologna, Il Mulino, 2009. G. Finocchiaro, (voce) *Identità personale (diritto alla*), cit., 729 ss.; E. Stradella, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella rete, quali anticorpi si possono sviluppare, e, infine cui prodest?*, in *Rivista AIC*, n. 4/2016, 22 s.; Aa.Vv., *Memoria versus oblio*, a cura di M. Bianca, Torino, 2019. Cfr. G. Bavetta, (voce) *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, Milano, 1970, 955; V. Zeno-Zencovich, *Travisamento (giudiziale) dell'identità personale*, in *Dir. dell'informazione e dell'informatica*, 1985, p. 686 ss.

[31] Si sottolinea che già negli anni '70, la giurisprudenza si era allontanata dall'idea di ricollegare l'identità personale soltanto ai c.d. "segni distintivi". Cfr. G. Bavetta, (voce) *Identità (diritto alla)*, in *Enc. dir.*, vol. XIX, Milano, 1970, 955.

[32] Ordinanza Pretura Verona 21-12-1982. Cfr., in dottrina, G. Pino, *Il diritto all'identità personale*, Il Mulino, Bologna, 2009.

zione civile e legale e l'immagine evoca le mere sembianze fisiche della persona, l'identità rappresenta, invece, una formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue specifiche caratteristiche e manifestazioni (morali, sociali, politiche, intellettuali, professionali, ecc.), cioè per esprimere la concreta ed effettiva personalità individuale del soggetto quale si è venuta solidificando od appariva destinata, in base a circostanze univoche, a solidificarsi nella vita di relazione». Pertanto, «il diritto all'identità personale mira a garantire la fedele e completa rappresentazione della personalità individuale del soggetto nell'ambito della comunità, generale e particolare, in cui tale personalità individuale è venuta svolgendosi, estrinsecandosi e solidificandosi»[33].

Appare, allora, chiaro che l'identità non possa essere ridotta a singoli tratti isolati, ma vada considerata nella sua globalità e complessità, rafforzando, così, l'idea che anche gli elementi culturali non siano meri attributi isolati della stessa, ma siano costitutivi della personalità del soggetto.

Occorre, inoltre, sottolineare che la tutela dell'identità personale, compresa la sua dimensione culturale – e, più in generale, ogni elemento caratterizzante l'identità personale – si estende anche alla dimensione *digitale* dell'identità[34]: l'identità digitale non si esaurisce, infatti, nella mera identificazione tecnica – garantita, ad esempio, da strumenti come SPID, carta d'identità elettronica, oppure, ancora altre credenziali elettroniche –, ma comprende anche aspetti ulteriori, che si intrecciano con la rappresentazione dell'identità personale nello spazio digitale.

Si precisa, infatti, che se, da una parte, il diritto all'identità personale in ambito digitale si lega al trattamento di quei cosiddetti "segni distintivi" (come il nome o l'immagine)[35], che permettono l'identificazione di un soggetto, dall'altra parte esso si estende *oltre* la mera *identificazione*, configurandosi come diritto alla *rappresentazione della personalità*, intesa quale riconoscimento della persona

---

[33] Cassazione civile, sent. n. 3769 del 22 giugno 1985 in *Foro it.*, cit.

[34] Cfr. G. Resta, *Identità personale e identità digitale*, ne *Il diritto dell'informazione e dell'informatica*, 2007, p. 511 ss.; G. Alpa, *L'identità digitale e la tutela della persona*, in *Contratto e impresa*, 2017, p. 723 ss.

[35] Sul tema, cfr. G. Resta, *Identità personale e identità digitale*, cit., p. 511 ss.

«nel complesso delle sue attività e delle sue posizioni professionali, culturali, ideologiche, religiose e sociali»[36].

In questi termini, allora, la rappresentazione della personalità del soggetto nello spazio digitale potrebbe, senza dubbio, ricomprendere anche elementi della sua identità culturale.

## 5. *Il rischio della profilazione algoritmica di tipo linguistico-culturale*

Pur non rientrando tra le categorie particolari di dati personali di cui all'art. 9 del GDPR – per le quali la profilazione è, in linea di principio, vietata[37] – è opportuno sottolineare come il trattamento dei dati personali di natura culturale possa comunque comportare rischi specifici di discriminazione linguistico-culturale e a sfondo razziale, soprattutto in relazione all'impiego di sistemi algoritmici e processi automatizzati di profilazione, intesa, ai sensi dell'art. 4 par. 4 del GDPR, come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[38]: con la locuzione

[36] V. ZENO-ZENCOVICH, (voce) *Identità personale*, cit., p. 294.

[37] Si ricorda, a tale proposito, che la profilazione dei dati cosiddetti sensibili è vietata ai sensi dell'art. 9 GDPR, salvo casi specifici enumerati nel paragrafo 2 del medesimo articolo – quali, a titolo esemplificativo, la presenza di un consenso esplicito al trattamento di tali dati; quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale; o, ancora, il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; oppure quando è necessario per motivi di interesse pubblico o di sanità pubblica.

[38] In altri termini, la profilazione rappresenta una tecnica di processamento automatico di dati personali (e talvolta non personali) finalizzata a sviluppare una conoscenza predittiva sotto forma di profili che possono, poi, essere applicati a singoli individui o gruppi per assumere decisioni. Cfr. Sulla definizione di "profilazione", G. MARX, N. REICHMAN. *Routinizing the Discovery of Secrets: Computers as Informants*, in *American Behavioral Scientist*, 27, 1984, 423 ss., L.A BYGRAVE, *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, The Hague,

di *machine profiling* si indica, poi, in particolare, quell'attività di profilazione svolta da sistemi algoritmici programmati da esseri umani, attraverso i quali la macchina elabora dati e restituisce informazioni strutturate.

In effetti, in ambito digitale, elementi come lingua, tradizioni, pratiche rituali, simboli o preferenze artistiche che costituiscono parte integrante dell'identità personale dell'interessato – e della sua rappresentazione in ambito digitale – diventano facilmente tracciabili e suscettibili di utilizzo nei processi di profilazione automatizzata.

Occorre, inoltre, precisare che le tecniche di profilazione algoritmica possono basarsi su dati *direttamente forniti dall'utente* (come, ad esempio, nell'ambito di dati personali di natura culturale, la madrelingua dichiarata o l'appartenenza a una minoranza culturale); *dati osservati* attraverso comportamenti online (playlist musicali, contenuti culturali seguiti, interazioni sui social); oppure *dati inferiti* tramite algoritmi (come l'appartenenza etnica, religiosa o culturale dedotta da modelli comportamentali digitali).

Nel caso dei dati personali di natura culturale, e considerando il ruolo centrale delle tecniche di identificazione e profilazione operanti nella rete, la profilazione tende a costruire una specifica rappresentazione culturale dell'interessato nell'ambiente digitale, con possibili rischi di discriminazione linguistico-culturale o, ancora, a sfondo razziale, soprattutto in determinati contesti quali l'accesso a contenuti, servizi o, ancora, opportunità lavorative. Ad esempio, discriminazioni linguistico-culturale potrebbero riguardare pubblicità mirata basata su dati culturali – come lingua, interessi culturali o appartenenza a determinate comunità etniche o minoranze – che potrebbe escludere alcuni gruppi dall'accesso a offerte di lavoro o corsi di formazione.

Anche i sistemi di *scoring* creditizio potrebbero integrare variabili legate a pratiche culturali o linguistiche, con il rischio di penalizzare comunità minoritarie nell'accesso a prestiti e servizi finanziari[39].

---

2002; M. HILDEBRANDT, *Who is Profiling Who? Invisible Visibility*, in S. GUTWIRTH *et al.* eds., *Reinventing Data Protection?*, Springer, Dordrecht, 2009, p. 239 ss.

[39] Sul tema delle implicazioni giuridiche derivanti dalla progressiva centralità delle tecniche di intelligenza artificiale in diversi settori pubblici e privati, si veda *ex*

In particolare, se la discriminazione costituisce una forma di differenziazione irragionevole tra situazioni analoghe o meritevoli di pari trattamento, emergono alcune criticità quando tali distinzioni non dipendono più da una condotta umana diretta, ma dal funzionamento di sistemi algoritmici. In questi casi, la discriminazione può derivare da processi decisionali automatizzati, nei quali il ruolo umano è ridotto o assente, e che si basano su meccanismi opachi e difficili da ricostruire *ex post*[40].

In aggiunta, quando attraverso dati personali di natura culturale diviene possibile inferire l'appartenenza dell'interessato a una determinata minoranza culturale o etnica, ovvero desumere elementi relativi all'orientamento sessuale, alle convinzioni filosofiche o ideologiche, il dato personale di carattere culturale potrebbe presentare dei rischi analoghi a quelli propri dei dati cosiddetti sensibili di cui all'art. 9 GDPR.

In tal senso, già il Considerando 71 del GDPR richiama espressamente l'esigenza di prevenire qualsiasi forma di discriminazione derivante da trattamenti automatizzati, connessa, tra l'altro, a dati riguardanti razza, origine etnica, opinioni politiche, religione, convinzioni filosofiche o appartenenza sindacale.

Analogamente, il Comitato europeo per la protezione dei dati (EDPB), nelle proprie *Linee guida sulla profilazione e sulle decisioni automatizzate*[41], ha sottolineato la necessità di adottare specifiche garanzie per evitare che l'utilizzo di algoritmi e tecniche di *machine learning*[42] possa comportare effetti discriminatori o pregiudizievoli per determinate categorie di persone[43].

---

*multis* A. Santosuosso, *Intelligenza artificiale e diritto*, Mondadori Università, Milano, 2020.

[40] J. Pearl, D. Mackenzie, *The book of why. The new science of cause and effect*, Basic Book, New York, 2018.

[41] *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251 rev.01) disponibile al link *https://ec.europa.eu/newsroom/article29/items/612053*.

[42] L. Califano, *Autodeterminazione vs. eterodeterminazione dell'elettore: voto, privacy e social network*, in *Federalismi.it*, n. 16, 2019, p. 3.

[43] G. Gaudio, *Le discriminazioni algoritmiche*, in *Lavoro, Diritti, Europa*, 1/2024. In generale, per esempi di discriminazioni algoritmiche, P.T. Kim, *Data-Driven Discrimination at Work*, in *Will. & Mary L. Rev.*, 58(3), 2016/2017, p. 857 ss.; P. Hacker,

Si precisa, infine, che forme di discriminazione linguistico-culturale potrebbero essere strettamente legate sia alla presenza di *bias*, ovvero di distorsioni di natura sistematica, che possono intervenire sia nella fase di programmazione, sia in quella di gestione del processo di apprendimento e dipendono dai dati selezionati e dai feedback forniti; sia all'utilizzo di algoritmi di *machine learning* che sono in grado di identificare caratteri c.d. "*proxy*", cioè variabili spesso apparentemente neutre che, tuttavia, dal punto di vista statistico/probabilistico, possono essere correlate ad un determinato fattore di discriminazione[44]: in questo caso, tali algoritmi potrebbero, allora, utilizzare come variabile rilevante nel processo decisionale un proxy diverso da un fattore di discriminazione che tuttavia appare statisticamente correlato a quest'ultimo, e che potrebbe produrre a "specchio"[45] un effetto discriminatorio.

## 6. *Il fenomeno della profilazione linguistico-culturale nei processi di gestione delle risorse umane*

In tale quadro, un ambito particolarmente sensibile a discriminazioni di tipo linguistico-culturale è quello relativo ai processi automatizzati di *recruitment* e gestione delle risorse umane. Spesso, infatti, per selezionare il personale vengono impiegati strumenti digitali e algoritmici (ad esempio piattaforme HR) che trattano dati personali potenzialmente idonei a rivelare l'appartenenza culturale di un candidato, come lingua madre, partecipazione ad associazioni culturali o appartenenza religiosa, etnica o nazionale, e che potrebbero penalizzare, ad esempio, candidati con nomi stranieri, lingue madri diverse da quella dominante o percorsi formativi presso isti-

*Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law*, in *Common Mkt. L. Rev.*, 2018, 55(4), p. 1143 ss.

[44] S. Renzi, *Decisioni automatizzate e analisi predittive e tutela della privacy dei lavoratori*, in *Lav. dir.*, n. 3, 2022, p. 593; L. Califano, *Tecnologie di controllo del lavoro, diritto alla riservatezza e orientamenti del Garante per la protezione dei dati personali*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017, pp. 165 ss.

[45] A. Lo Faro, *Algorithmic Decision Making e gestione dei rapporti di lavoro: cosa abbiano imparato dalle piattaforme*, in *Federalismi.it*, 5 ottobre 2022, pp. 195-197.

tuzioni culturalmente marginali, replicando pregiudizi culturali già esistenti nell'ambiente offline.

Si menziona, a titolo esemplificativo, il caso emblematico di Amazon del 2015[46] che aveva progettato e utilizzato un algoritmo per i processi di reclutamento del personale che discriminava il genere femminile, sulla base di una profilazione fondata anche su dati personali di natura culturale.

L'effetto discriminatorio del processo decisionale era, in particolare, conseguenza della capacità dell'algoritmo di identificare una serie di caratteri, essenzialmente legati all'identità di genere, ma anche a preferenze culturali e appartenenze culturali correlati al genere dei candidati, e di utilizzarli poi come variabili rilevanti ai fini della decisione: ad esempio far parte di determinate associazioni culturali o aver frequentato determinate scuole costituiva un dato che l'algoritmo aveva imparato a correlare, poi, al genere.

Un'altra forma di discrimnazione nell'ambito della selezione del personale è la cosiddetta *linguistic profiling*[47], fenomeno di carattere emergente, che si riferisce, in particolare, all'utilizzo di strumenti digitali, algoritmi e sistemi di intelligenza artificiale per analizzare il linguaggio di un candidato al fine di valutare caratteristiche personali, competenze professionali o affinità linguistico-culturali.

Tale analisi riguarda sia il linguaggio scritto (come CV, lettere di presentazione, email e chat), sia quello orale, inclusi colloqui-video, e comprende l'analisi di stile, lessico, sintassi, tono e scelte linguistiche. Gli obiettivi della profilazione linguistica nell'ambito del *recruitment* includono la selezione e il ranking dei candidati attraverso, ad esempio, algoritmi di scoring.

I metodi impiegati nel *linguistic profiling* possono avvalersi del *Natural Language Processing* (NLP)[48], che può essere utilizzato per

---

[46] Cfr. sul caso Amazon, J. Dastin, *Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, 11 ottobre 2018; G. Gaudio, *Le discriminazioni algoritmiche*, cit.

[47] Cfr. M. Bucholtz, K. Hall, *Identity and interaction: A sociocultural linguistic approach*, in *Discourse Studies*, vol. 7(4-5), 2005, p. 585 ss. Sul tema, cfr. Anche M.T. Turell, *The forensic linguistic implications of authorship attribution*, in *International Journal of Speech, Language & the Law*, vol. 9, 2020, pp. 211 ss.

[48] S. Devaraju, *Natural Language Processing (NLP) in AI-Driven Recruitment*

identificare caratteristiche culturali, preferenze o atteggiamenti degli individui attraverso l'analisi di testi, messaggi o altri contenuti digitali; oppure di sistemi di *voice analytics*, che analizzano elementi paralinguistici come tono, intonazione e pronuncia durante i colloqui, al fine di estrarre informazioni sul profilo personale, culturale o emotivo del candidato: tali strumenti potrebbero, allora, rivelare caratteristiche identitarie o appartenenze culturali, aumentando i rischi di profilazione e discriminazione nell'ambito delle pratiche di selezione del personale, penalizzando, ad esempio, candidati in base a dati riguardanti la lingua madre, l'accento, la scelta di parole o lo stile comunicativo e rischiando di comportare un trattamento differenziato su base culturale, etnica o linguistica.

In particolare, alcuni recenti studi[49] che hanno esaminato i *bias* nei colloqui di lavoro connessi all'accento dei candidati nell'utilizzo della lingua inglese, dimostrano come i candidati di lingua inglese con accento "non standard" ricevano valutazioni significativamente inferiori in termini di competenza e idoneità all'assunzione rispetto a coloro che parlano con un accento percepito come standard. In alcuni casi, l'analisi dei colloqui mediante algoritmi di *machine learning* può portare all'attribuzione di punteggi inferiori ai candidati il cui accento sia percepito come "non madrelingua inglese", anche quando il messaggio risulti chiaro e comprensibile. Tale meccanismo potrebbe tradursi in esclusioni sistematiche dai processi di selezione del personale, evidenziando dei rischi di discriminazione insiti nell'uso di strumenti automatizzati di valutazione dei candidati.

## 7. *La regolazione della profilazione linguistico-culturale nel GDPR.*

La crescente diffusione di processi automatizzati di profilazione, pur regolati dallo stesso GDPR nell'ambito del trattamento

---

*Systems*, in *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, Vol. 8, Issue 3, 2022.

[49] W. A. Albassam, *The power of artificial intelligence in recruitment: an analytical review of current ai-based recruitment strategies*, in *International Journal of Selection and Assessment*, n. 5/2023; P. Cappelli, P. Tambe, V. Yakubovich, *Artificial Intelligence in Human Resources Management: Challenges and a Path Forward*, in *Electronic Journal*, 2018; A. Gupta, M. Mishra, *Ethical Concerns While Using Artificial Intelligence in Recruitment of Employees. Business Ethics and Leadership*, 6(2), 2022, p. 6 ss.

dei dati personali, solleva questioni di rilievo giuridico con riferimento tanto alla tutela dei dati personali trattati previsto dall'art. 8[50] della Carta Europea dei diritti fondamentali dell'Unione e tutelato anche dall'ordinamento costituzionale italiano, quanto al rispetto del principio di non discriminazione previsto dall'art. 21 della riferita Carta, nonché dall'art. 3 Cost.

Innanzitutto, sulla base della disciplina prevista dal GDPR, se, come già sottolineato, per i dati personali appartenenti a "categorie particolari" vige un divieto generale di trattamento, i dati personali di carattere culturale, al contrario, non solo non rientrano tra le categorie particolari di dati, ma non è prevista all'interno del GDPR alcuna norma specifica che ne disciplini il trattamento e in particolare il trattamento per finalità di profilazione automatizzata: nel caso di dati personali di natura culturale, si applicano, pertanto, le regole generali dettate dal GDPR in materia di trattamento dei dati personali, con riguardo alla profilazione automatizzata.

In particolare, rispetto alla profilazione, e ad ogni altro trattamento automatizzato che si avvalga di dati personali, il GDPR prevede all'art. 15 il diritto di ottenere informazioni circa la logica utilizzata, l'importanza e le conseguenze di tale trattamento per l'interessato. Ai sensi dell'art. 15 del riferito Regolamento, l'interessato ha diritto di ottenere dal titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano. Se i dati sono trattati, l'interessato può accedere ai dati personali oggetto di trattamento e ricevere le seguenti informazioni: finalità del trattamento; categorie di dati trattati; destinatari o categorie di destinatari a cui i dati sono stati comunicati (inclusi destinatari in paesi terzi/organizzazioni internazionali); periodo di conservazione previsto o criteri usati per determinarlo; esistenza dei diritti di rettifica, cancellazione, limitazione, opposizione; diritto di proporre reclamo a un'autorità di controllo; origine dei dati (se non raccolti direttamente dall'interessato); esistenza di processi decisionali automatizzati, inclusa la profilazione, con informazioni "significative" sulla logica utilizzata, nonché sull'importanza e le conseguenze previste per l'interessato.

[50] Carta dei diritti fondamentali dell'UE , Articolo 8, par. 1 «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano».

È, in particolare, quest'ultima previsione dell'art. 15 a configurare un cosiddetto *right to explanation*, ovvero un diritto a comprendere la funzionalità del sistema, cioè la logica, il significato, le conseguenze previste e la funzionalità generale di un sistema di decisione automatizzata, quali, ad esempio, le specifiche dei requisiti del sistema, gli alberi decisionali, i modelli predefiniti, i criteri e le strutture di classificazione[51].

Come osservato, le informazioni *significative* che devono essere fornite agli interessati sulla logica, sull'importanza e sulle conseguenze del processo decisionale ai sensi dell'art. 15 del riferito Regolamento «dovrebbero essere intese come la "leggibilità' dell'"architettura" e dell'"implementazione" del trattamento algoritmico»[52] e dovrebbero garantire la cosiddetta *legibility* del procedimento algoritmico, intesa come esigenza di *trasparenza*[53], da concepirsi tanto come *spiegabilità* del processo decisionale sotteso agli algoritmi, quanto come *possibilità effettiva di comprenderne i meccanismi operativi*, «ovvero come modo in cui la decisione è stata presa in relazione alla specifica situazione soggettiva e fattuale dell'interessato»[54].

Anche l'art. 22 GDPR regola l'ambito della profilazione: tale norma vieta che determinate decisioni con effetti significativi sulla sua persona siano completamente automatizzate, prevedendo, pertanto, l'intervento umano. Il primo paragrafo dell'art. 22 chiarisce, infatti, che «l'interessato ha il diritto di non essere sottoposto a una

---

[51] S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017; M. Palmirani, *Big Data e conoscenza*, in *Rivista di filosofia del diritto*, 2020, p. 73 e ss.

[52] G. Malgieri, G. Comandé, *Why a right of legilibility*, in *International Data Privacy Law*, vol. 7, n. 4, 2017, p. 243 ss.

[53] A. Simoncini, *Profili costituzionali dell'amministrazione algoritmica*, in *Rivista Trimestrale di Diritto Pubblico*, n. 3, 2019.

[54] G. Resta, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza* in *Politica del diritt*o, 2019, p. 228. Come osservato, permane in linea generale la denuncia del carattere oscuro degli algoritmi che diventa il punto di riflessione della dottrina pubblicistica intanto questi risultano essere vere e proprie scatole nere, per la difficoltà di addentrarsi nei meccanismi che presiedono il lo funzionamento, soprattutto per quei sistemi che utilizzano una grande quantità di dati e che, talvolta, che non si limitano a seguire istruzione, ma trovano soluzioni e percorsi inediti. O. Pollicino, *Regolazione e innovazione tecnologica nell'ordinamento della rete*, in *Riv. AIC*, n. 2, 2025, p. 152 ss.

decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

Tuttavia, il diritto di opporsi ai procedimenti di decisione automatizzata risulta cedevole in presenza delle tre ipotesi di esclusione previste dal secondo paragrafo dell'art. 22 del GDPR. Tali eccezioni riguardano i casi in cui la profilazione o la decisione automatizzata siano: necessarie per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento; autorizzate dal diritto dell'Unione o degli Stati membri, purché accompagnate da misure adeguate di tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; oppure fondate sul consenso esplicito di quest'ultimo.

In ogni caso, il paragrafo 3 dell'art. 22 precisa che, anche qualora ricorra una delle ipotesi previste dal secondo paragrafo, il titolare del trattamento è comunque tenuto ad adottare «misure appropriate per tutelare i diritti, libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione»[55].

Appare, invece, assente, nell'impianto normativo del GDPR, un riferimento esplicito e puntuale al principio di non discriminazione[56], limitandosi, il testo del riferito Regolamento, ad un richiamo piuttosto vago e generico ad un principio di "prevenzione" dei potenziali effetti discriminatori di trattamenti automatizzati, previsto dallo stesso GDPR al Considerando 71[57].

---

[55] AA.VV., *AI: profili giuridici Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, n. 3, 2019, p. 15.

[56] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, cit., p. 84.

[57] Cfr. Considerando (71) del GDPR: «Al fine di garantire un trattamento corretto e trasparente in relazione all'interessato, il titolare del trattamento dovrebbe utilizzare procedure matematiche o statistiche appropriate, attuare misure tecniche e organizzative adeguate per garantire, in particolare, che siano corretti i fattori sui quali si basano i dati personali e ridurre al minimo il rischio di errori, garantire la sicurezza dei dati personali e prevenire effetti discriminatori nei confronti delle persone fisiche per motivi di razza o origine etnica, opinioni politiche, religione o convinzioni, appartenenza sindacale, stato genetico o sanitario o orientamento sessuale, o per effetto della

## 8. *Profilazione "culturale" e disciplina prevista dal DSA*

Accanto, poi, al GDPR, è opportuno menzionare – sebbene non sia possibile approfondirne in questa sede l'analisi – il Regolamento (UE) 2022/2065, noto come *Digital Services Act* (DSA), il quale introduce, nell'ambito del più ampio quadro degli obblighi imposti ai prestatori di servizi digitali, disposizioni volte a disciplinare il trattamento dei dati personali nei processi automatizzati, quali la profilazione e raccomandazione dei contenuti.

Il DSA interviene, in particolare, al fine di prevenire e mitigare i potenziali effetti discriminatori derivanti dall'uso degli algoritmi, ponendo l'accento sul principio di trasparenza (art. 27 del riferito Regolamento): si impone, invero, ai prestatori di servizi digitali di informare in modo chiaro gli utenti sui criteri utilizzati per la personalizzazione dei contenuti e sulla logica di funzionamento degli algoritmi che ne determinano la visibilità[58].

In aggiunta, secondo una logica incrementale *risk based* relativa agli obblighi previsti per i prestatori di servizi digitali[59], il DSA prevede per le piattaforme online di dimensioni molto grandi e i motori di ricerca online di dimensioni molto grandi un *obbligo di valutazione* (art. 34)[60] e di *attenuazione* (art., 35) dei cosiddetti rischi sistemici nell'Unione derivanti dalla progettazione o dal funzionamento del loro servizio e dei relativi sistemi, compresi i sistemi algoritmici: rischi quali eventuali effetti negativi, attuali o prevedibili, per l'esercizio dei diritti fondamentali, tra cui il mancato rispetto del principio di non discriminazione[61].

Di rilievo è, inoltre, il divieto posto dall'art. 26, par. 3, di ricorrere alla profilazione basata su categorie particolari di dati per-

---

profilazione. Le decisioni automatizzate e la profilazione basate su categorie particolari di dati personali dovrebbero essere consentite solo a determinate condizioni».

[58] M. Orofino, *Il Digital Services Act tra continuità (solo apparente) e innovazione*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea della società digitale*, cit., p. 153.

[59] E. Longo, *La disciplina del "rischio digitale"*, in S. Calzolaio, A. Iannuzzi, E. Longo, M. Orofino, F. Pizzetti, *La regolazione europea della società digitale*, cit.

[60] Per un approfondimento su tale disposizione, si veda V. Colaricco, M. Cogode, *Gli obblighi applicabili a piattaforme online di dimensioni molto grandi (Artt. 33-43)*, in *Diritto di Internet*, n. 1, 2023, p. 27 ss.

[61] Cfr. art. 34, par. 1, lettera *b*) del DSA.

sonali ai sensi dell'art. 9 GDPR, quali quelli idonei a rivelare l'origine etnica, le convinzioni religiose o filosofiche e l'orientamento sessuale. Tale previsione rafforza la tutela già riconosciuta dal GDPR, estendendola all'ambito della regolazione dei servizi digitali, ove la raccolta dei dati avviene su larga scala e anche attraverso processi automatizzati di cosiddetta inferenza.

Non si possono, poi, trascurare i poteri attribuiti alla Commissione Europea dal *Digital Services Act* per la supervisione nell'applicazione della disciplina prevista, l'investigazione e la sanzione, specialmente nei casi relativi ai *Very Large Online Platforms* (VLOPs) e *Very Large Online Search Engines* (VLOSEs)[62]: l'art. 65 e l'art. 66 del DSA prevedono rispettivamente in capo alla Commissione poteri di indagine sul rispetto, da parte dei fornitori di piattaforme e motori online di grandi dimensioni, di tutti gli obblighi previsti dal Regolamento e il potere di avviare un procedimento nel caso la Commissione abbia il sospetto che un obbligo sia stato violato. A tal fine il Regolamento attribuisce alla Commissione poteri di audizione e di raccolta informazioni, poteri ispettivi e poteri correttivi inclusi quelli sanzionatori[63].

## 9. *Addestramento dei sistemi di AI e rappresentatività dei dati di natura culturale*

Infine, anche l'*AI Act* assume un rilievo significativo nella regolazione della profilazione prodotta da sistemi di intelligenza artificiale, introducendo un approccio basato sul rischio per la valutazione dei sistemi di *AI.* L'art. 5 vieta, infatti, esplicitamente i sistemi di *AI* che impiegano tecniche di manipolazione cognitiva o che sfruttano vulnerabilità legate, tra l'altro, all'età, alla disabilità o alla condizione sociale e *culturale* dell'individuo.

Inoltre, si rileva che anche i sistemi di *AI* utilizzati per la *profilazione linguistico-culturale* potrebbero rientrare tra quelli cosid-

[62] M. Orofino, *Il Digital Services Act tra continuità (solo apparente) e innovazione*, cit., p. 169 ss.

[63] V. M. Pavese, *Commissione: ruolo, poteri, disciplina applicabile*, in L. Bolognini, E. Pelini, M. Scialdone (a cura di), *Digital Service Act e Digital Market Act*, cit., p. 179 ss.

detti a "rischio elevato", richiedendo pertanto una valutazione d'impatto sui diritti fondamentali e l'adozione di misure di mitigazione dei *bias* algoritmici.

Al considerando 29 del Regolamento, si pone, poi, l'attenzione su quei sistemi di intelligenza artificiale che possono sfruttare le vulnerabilità di una persona o di uno specifico gruppo di persone, tra cui le minoranze etniche o religiose, con l'obiettivo o l'effetto di influenzare il comportamento di una persona e in un modo che provochi o possa verosimilmente provocare a tale persona o a un'altra persona o gruppo di persone un danno significativo, chiarendo che tali sistemi dovrebbero essere vietati.

L'art. 10 dell'AI Act stabilisce, infine, che i dati utilizzati per l'addestramento, la validazione e il testing dei sistemi di IA ad alto rischio debbano essere, oltre che accurati, anche *rappresentativi*. La rappresentatività dei dati è fondamentale affinché si riduca il rischio che il sistema impari *pattern* discriminatori, in quanto i sistemi automatizzati alimentati con dati non sufficientemente diversificati tendono a privilegiare soggetti o gruppi già sovrarappresentati e a penalizzare individui o gruppi marginalizzati.

In aggiunta, la rappresentatività dei dati nell'addestramento dei sistemi di AI assume una dimensione significativa anche rispetto alla tutela del pluralismo culturale: se i dati di *training* riflettono un ambito culturale molto ristretto, il sistema di IA potrebbe reiterare un modello culturale egemone, marginalizzando espressioni identitarie differenti.

In questo senso, la rappresentatività costituisce un elemento essenziale per garantire l'affidabilità e la non discriminazione dell'output generato dal sistema e si configura non solo quale presupposto tecnico-operativo, ma assume anche una rilevanza sul piano della tutela dei diritti fondamentali[64].

## 10. *Conclusioni*

Sebbene i dati personali di natura culturale abbiano acquisito crescente rilevanza in ambito digitale, tuttavia, il GDPR non forni-

[64] Cfr. M. Orofino, *Obiettivi, ambito di applicazione e principi fondamentali dell'AI*, cit., p. 51 ss.

sce una definizione esplicita di dato culturale, pur considerando gli elementi dell'identità culturale tra i fattori che potrebbero rendere una persona identificabile e suscettibili di tutela: si evidenzia, pertanto, uno spazio di "zona grigia" nell'ambito della definizione di tali dati, che pur incidono in modo significativo sulla sfera identitaria dell'individuo, nonché sulla sua rappresentazione nello spazio digitale.

Il Legislatore europeo potrebbe, allora, intraprendere uno sforzo di carattere definitorio, volto a delineare la categoria di "dati personali di natura culturale", riconoscendone la specificità e la crescente rilevanza nel contesto digitale: ciò risulterebbe particolarmente significativo alla luce delle recenti evoluzioni normative in materia di protezione e circolazione dei dati, volte, in particolare, alla creazione di nuovi spazi condivisi di dati culturali, finalizzati a tutelare il patrimonio culturale materiale e immateriale dell'Unione Europea.

In questo quadro, emerge, inoltre, la necessità di una valutazione sull'eventuale previsione, da parte del Legislatore europeo, e con riferimento a casi specifici – quando, ad esempio, attraverso i dati personali di natura culturale è possibile inferire dati appartenenti a categorie particolari ai sensi dell'art. 9 GDPR –, di una tutela *rafforzata* dei dati personali di natura culturale: questo, soprattutto nell'ambito della profilazione automatizzata e dei sistemi di intelligenza artificiale, prevedendo un intervento umano, qualora le decisioni basate sul trattamento automatizzato a cui può essere sottoposto l'interessato producano effetti giuridici che lo riguardano o che incidano significativamente sulla sua persona.

Come evidenziato, l'impiego di dati personali di carattere culturale nei processi di profilazione linguistico-culturale comporta, infatti, rischi particolarmente importanti di discriminazione diretta e indiretta, con riferimento ad esempio nell'accesso a opportunità lavorative o a servizi, che potrebbero tradursi in forme di discriminazione a sfondo razziale o culturale.

Infine, se è vero che, da un lato, le norme previste dal GDPR e introdotte, più recentemente, dal DSA e dall'AI Act intervengono nella mitigazione dei rischi di discriminazione, anche nell'ambito di quella linguistico-culturale, dall'altro lato permane, in ogni caso,

una sfida di carattere strutturale, connessa, in particolare, alla *trasparenza* degli algoritmi, che operano spesso su logiche complesse e opache, non sempre riconducibili a schemi di controllo tradizionali[65].

In questo senso, il c.d. *right to know*[66] dovrebbe assumere un rilievo sempre maggiore in quanto strumentale e decisivo ai fini dell'accertamento dell'eventuale *agere* discriminatorio dell'algoritmo[67] nell'ambito specifico dei sistemi di profilazione e, più in generale, nella governance dell'intelligenza artificiale.

---

[65] A. Celotto, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi Giuridica dell'Economia*, n. 1, 2019, p. 47 ss.

[66] M. Palmirani, *Big Data e conoscenza*, in *Rivista di filosofia del diritto*, 2020, 73 e ss.

[67] C. Nardocci, *Intelligenza artificiale e discriminazioni*, in *Convegno annuale dell'associazione "Gruppo di Pisa" Il diritto costituzionale e le sfide dell'innovazione tecnologica 18 e 19 giugno 2021*, fasc. 3/2021, p. 54 ss.

ANDREA RUFFO

# LE *BIG TECH* E LE NUOVE TECNOLOGIE CRITICHE: DALLA REGOLAZIONE ALL'AUTONOMO SVILUPPO INTERNO UE

SOMMARIO: 1. L'Europa e la sfida delle tecnologie digitali: tra regolazione del mercato e Sicurezza. – 2. Le nuove tecnologie critiche. – 3. L'obiettivo della sovranità tecnologica dell'UE. – 4. Il quadro normativo di riferimento. – 5. Approcci alla regolazione delle nuove tecnologie critiche per la sicurezza cibernetica UE. – 6. Conclusioni.

## 1. *L'Europa e la sfida delle tecnologie digitali: tra regolazione del mercato e Sicurezza*

Lo sviluppo esponenziale e incessante delle tecnologie digitali della rete Internet, prodottosi negli ultimi quindici anni, e il correlato impatto sull'economia e sulla finanza di settore (c.d. *Fintech*), hanno influenzato notevolmente il perimetro definitorio e operativo della sicurezza nazionale.

Se in precedenza l'azione di vigilanza e prevenzione dello Stato, anche in campo economico-finanziario, si sviluppava sui domini "classici" (di terra, mare, aria e spazio), dal primo decennio del XXI sec., l'uso preponderante della Rete e la crescente interconnessione dei mercati, ha reso indispensabile il monitoraggio della dimensione tecno-economica-cibernetica.

Questo slittamento d'attenzione, dallo spazio fisico a quello digitale, impone una rilettura di alcune categorie del diritto pubblico e, quindi, del d. costituzionale.

L'emergere della realtà digitale ha ampliato, in tutti i sensi, i confini del concetto di sicurezza, non solo moltiplicando le minacce per lo Stato (confondendo gli attori e gli obiettivi delle condotte

malevole) ma anche rendendo ancor più poliedrico e volatile il panorama dei fattori di influenza e condizionamento esterno (diretto o indiretto); dall'ambito economico-commerciale a quello finanziario-monetario[1].

In questo contesto, il rapporto tra Stato e imprese private (produttrici di tecnologie digitali) assume un'importanza crescente, tanto – in ambito di regolazione dell'economia – nel garantire i principi a tutela del mercato e i diritti dei cittadini (produttori/consumatori), quanto – in ottica pubblicistica – nel concorrere alla sicurezza nazionale, nonché nell'influenzarne i rapporti economico-finanziari.

L'attuale contesto normativo europeo, profondamente influenzato nel 2020 dalla pandemia da Covid-19 e dalla conseguente ripresa socio-economica, nonché dal successivo conflitto russo-ucraino (in corso dal 2022), ha visto la nascita di una serie di misure regolatorie, volte a incentivare e a rafforzare l'assetto economico digitale UE. Ne sono da esempio i regolamenti del c.d. "pacchetto digitale" (DMA[2], DSA[3] e DGA[4]), di cui il GDPR[5] fu – in parte – precursore, così come il successivo Regolamento IA e, in ambito finanziario, il MICAR[6]. Misure normative europee di sviluppo e tutela del mercato digitale che si affiancano ad altri provvedimenti (come le direttive NIS I e II, le misure di controllo sugli investimenti esteri[7], le c.d. "*golden power*" e, da ultimo, il Piano UE "*Readiness*"2030[8]), volti a potenziare la sicurezza delle infrastrutture e tecnologie digitali interne, rispetto ad ingerenze o a investimenti esteri potenzialmente ostili.

In un'economia digitale dominata dal sostanziale oligopolio dalle imprese multinazionali d'Oltreoceano (statunitensi), riassumi-

---

[1] H. Farrell, A.L Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, in *International Security*, 44(1), 2019.

[2] "*Digital Market Act*"; Reg. (UE) 2022/1925.

[3] "*Digital Service Act*"; Reg. (UE) 2022/2065.

[4] "*Data Governance Act*"; Reg. (UE) 2022/868.

[5] "*General Data Protection Regulation*"; Reg. (UE) 2016/679.

[6] "*Markets in Crypto-Assets Regulation*"; Reg. (UE) 2023/1114.

[7] Definite *nell'EU Foreign Direct Investment* (FDI) *screening framework*.

[8] Specificamente per il potenziamento e la promozione dell'autonomia strategica europea, nel campo delle tecnologie di droni e cyber-sicurezza, così come di quelle emergenti di intelligenza artificiale e fisica quantistica.

bili nell'acronimo "GAMAM" (Google, Apple, Meta, Amazon, Microsoft), in competizione con i colossi tecnologici cinesi (Alibaba, Huawei, TikTok e Zhejiang), il Vecchio Continente recita il ruolo del consumatore ideale, completamente dipendente dai servizi *cyber-tech* a buon mercato e incapace di esercitare un qualsiasi tipo di competizione.

Con le ultime misure di regolazione, quindi, le istituzioni europee intenderebbero, da una parte, promuovere il mercato digitale, garantendo il libero accesso alle piccole imprese interne, in un regime di concorrenza leale con le Grandi (sottoposte, a loro volta, al rispetto dei valori dell'Unione), dall'altra, "proteggere" lo sviluppo delle aziende UE, per promuovere la sovranità tecnologica e limitare la dipendenza da fornitori statali o privati esteri, con la conseguente penetrazione nel mercato comune delle loro tecnologie "critiche".

A tutto questo si deve aggiungere che, con il piano di incremento della difesa europea (tracciato dal "*Readiness* 2030") si pone, l'ulteriore intento di potenziare il comparto militare dell'UE, seppur nel breve-medio periodo, mediante l'ineludibile dipendenza dall'industria bellica statunitense e dalle realtà produttrici di sistemi d'arma e *software* collegate (in alcuni casi anche israeliane o di paesi del *Commonwealth*). Aspetto che, oltre ad alimentare l'irraggiungibile dominanza commerciale delle produzioni extraeuropee, a detrimento di qualsiasi possibilità di sviluppo interno e leale concorrenza sul mercato[9], contribuirà a perpetuare l'immissione nello scenario UE di tecnologie critiche (alla base ad esempio di molti software di sicurezza e supporto militare), non totalmente padroneggiabili dai 27 Stati membri o, meglio, facilmente controllabili dall'esterno dai loro produttori.

Si è, pertanto, in una situazione cruciale per la stessa sopravvivenza degli obiettivi dell'Unione europea dell'ultimo decennio, in cui sussistono – dettate dalle contingenze geopolitiche e dall'incessante sviluppo delle tecnologie – esigenze plurime da soddisfare con condotte contrapposte[10].

---

[9] Con l'esclusione di alcuni settori in cui le industrie UE detengono meritevoli primati, almeno qualitativi.

[10] G. Ghidini, *Grandi piattaforme digitali e libera informazione: le difese europee*, in *Analisi Giuridica dell'Economia*, n. 2/2024, p. 3 e ss.

In un contesto di continuo progresso tecnologico, alimentato soprattutto da realtà economiche extraeuropee i tentativi di regolazione dell'UE (sia in ottica commerciale che securitaria) rischiano di risultare tardivi e, in alcuni, anche casi controproducenti; più d'ostacolo per gli stessi europei che per le entità estere.

Le c.d. GAMAM, anche note come Big Tech, nella loro totalità extra-europee (statunitensi), forti del loro oligopolio nel controllo dei servizi digitali sulla rete Internet, tendono comunque a condizionare – nonostante i provvedimenti sanzionatori e regolatori di Bruxelles e degli Stati membri – le politiche e le società dei 27 Paesi UE. Il tradizionale rapporto tra sicurezza nazionale-libertà di mercato si arricchisce di una dimensione nuova, in cui gli attori non sono più solo Stati sovrani, ma anche entità private transnazionali – le Big Tech – il cui potere economico, infrastrutturale e di dati spesso sorpassa quello di molte nazioni. Il potere economico dominante tende necessariamente, per mantenersi ed accrescersi, a imporsi anche nella sfera della politica e dell'attività istituzionale, dando vita a nuove forme di *regulatory capture*[11] tra poteri economici e politici. La regolazione giuridica dell'economia assume, in questo contesto, un'importanza crescente, tanto nel garantire i principi a tutela del mercato e i diritti dei cittadini[12], quanto nel concorrere alla sicurezza nazionale.

Di fronte a tale ardua sfida, l'Europa emerge come attore principale, elaborando una risposta normativa che impone una duplice riflessione. Questa, infatti, non solo verte sulla tipologia di strumento da adottare, ma ripropone anche l'attualità delle categorie tradizionali del costituzionalismo liberal-democratico, ora calate in una dimensione virtuale che ne stravolge i rapporti tra pubblico e privato[13].

---

[11] Comportamento per cui un'agenzia di regolamentazione, invece di agire per l'interesse pubblico, finisce per essere influenzata o controllata dalle stesse industrie o dagli interessi che dovrebbe regolare. Così facendo favorisce le aziende e i settori a cui è preposto il controllo, portando a decisioni che danneggiano il benessere collettivo (aumento prezzi e minore innovazione).

[12] V. M. Bassini, *Fundamental rights and private enforcement in the digital age*, in *European Law Journal*, vol. 25, Issue n. 2, 2019, p. 187.

[13] L. Floridi, *The European Legislation on AI: A Brief Analysis of its Philosophical Approach*, in *Philosophy & Technology*, 34, June 2021, p. 220.

## 2. *Le nuove tecnologie critiche*

Proprio questa riconfigurazione del rapporto tra pubblico e privato, resa ancor più tangibile nella dimensione digitale, non è un'evoluzione astratta, ma una diretta conseguenza del peso strategico acquisito da tali strumenti nella società. In altri termini, la necessità di ripensare gli assetti tradizionali del diritto scaturisce, in modo impellente, dal fatto che le tecnologie si configurano come l'epicentro della competizione geopolitica ed economica contemporanea. La duplice riflessione sulla scelta degli strumenti e sull'adeguatezza delle categorie giuridiche non avviene nel vuoto, bensì nel concreto contesto di una corsa globale per la supremazia tecnologica in cui, le c.d. "tecnologie critiche" rappresentano un polo della competizione geopolitica ed economica contemporanea.

La definizione "tecnologie critiche" non designa semplicemente degli strumenti avanzati, ma identifica un preciso insieme di beni, conoscenze e infrastrutture digitali la cui disponibilità, integrità e sicurezza sono considerate fondamentali per la sopravvivenza di uno Stato (e, pertanto, anche della stessa Unione Europea) come entità politica, economica e strategica. Tale importanza si manifesta nel loro duplice e contemporaneo ruolo di motore di prosperità economica nel mercato unico ed di elemento imprescindibile della sicurezza nazionale. Ai sensi del Regolamento (UE) 2019/452, che delinea un quadro normativo di controllo degli investimenti diretti esteri, le tecnologie critiche sono quelle la cui acquisizione o controllo da parte di soggetti extraeuropei potrebbe pregiudicare la sicurezza o l'ordine pubblico. La rilevanza strategica di tali beni è determinata, quindi, dalla dipendenza da essi dei servizi essenziali e delle attività economiche fondamentali (dai settori energetico e sanitario a quello finanziario)[14]. La qualifica di "criticità", infatti, travalica la mera funzione difensiva dello "*screening*" degli investimenti.

Una tecnologia è giuridicamente qualificabile come "critica" in base a una serie di criteri cumulativi. In primo luogo, deve posse-

[14] Parlamento Europeo, Dipartimento per le Politiche delle Relazioni Esterne, *The European space sector as an enabler of EU strategic autonomy*, 2020.

dere un carattere abilitante e trasversale, ossia deve costituire una base tecnologica abilitante fondamentale[15] per molteplici settori industriali e servizi essenziali. Rientrano in questa categoria l'intelligenza artificiale, le tecnologie quantistiche, i semiconduttori, le reti di telecomunicazione 5G e 6G, nonché le tecnologie spaziali. In secondo luogo, la tecnologia deve essere strategicamente rilevante, nel senso che la dipendenza da fornitori esteri crea una vulnerabilità sistemica per la resilienza economica e la sicurezza dell'Unione. Terzo, molte di queste tecnologie presentano una natura *dual-use*, essendo impiegabili sia per applicazioni civili e commerciali che per scopi di difesa, sicurezza e intelligence, che ne accentua ulteriormente l'importanza strategica.

Per tutto questo, le implicazioni giuridiche della predetta classificazione sono profonde e concrete. La qualifica di tecnologia critica determina la sua soggezione a un rigoroso scrutinio in caso di investimenti esteri, la priorità nell'accesso a finanziamenti europei dedicati[16]e l'inclusione in piani industriali e di ricerca volti a costruire l'autonomia strategica dell'UE.

Con la nuova proposta di regolazione della Commissione europea 837/2025[17] definita "*Digital Omnibus*", per i molteplici interventi di aggiornamento e modifica di svariati regolamenti UE nell'ambito digitale, si prevede anche di facilitare l'innovazione anche rispetto alle tecnologie critiche, semplificando le norme sulla condivisione dei dati e chiarendo le condizioni per il elaborazione e implementazione dei sistemi di IA[18].

Salvo che nelle tecnologie di calcolo quantistico in cui si registrano centri di assoluta avanguardia (italiana ed europea[19]), l'UE registra un significativo ritardo nello sviluppo e nello studio di tutte le alte tecnologie critiche.

---

[15] In inglese "*Key Enabling Technology*" (KET).

[16] Come quelli del programma Europa Digitale o di Horizon Europe.

[17] Proposta COM(2025) 837, pubblicata dalla Commissione europea il 19 novembre 2025.

[18] Attraverso anche modifiche mirate all'impianto normativo del GDPR.

[19] Si fa riferimento al DAMA Tecno-polo di Bologna, centro per il calcolo quantistico, coordinato da Cineca e parte del progetto nazionale ICSC (Centro Nazionale di ricerca in HPC, Big Data e Quantum Computing).

Non è un caso, infatti, che proprio relativamente alle tecnologie critiche, il Regolamento (UE) 2019/452 abbia introdotto un quadro europeo per il controllo degli investimenti esteri diretti per cui ogni Stato membro ha facoltà di valutare se un investimento nel proprio territorio possa pregiudicare l'ordine pubblico e la sicurezza. In prospettiva, infatti, la proposta "*Digital Omnibus*" introdurrebbe misure per proteggere i segreti commerciali europei dalla divulgazione a entità di paesi terzi con sistemi di protezione insufficienti, rafforzando la capacità dell'UE di custodire il proprio patrimonio tecnologico[20].

Un ritardo particolarmente significativo per l'Unione Europea si registra nel settore delle telecomunicazioni. La forte dipendenza tecnologica dell'UE per l'erogazione di servizi attraverso le reti 5G genera una condizione di vulnerabilità strutturale. Tale affidamento su tecnologie di provenienza inizialmente cinese comporta, inoltre, dirette implicazioni per la sicurezza dell'Unione, esponendo gli Stati membri, più che in passato, al rischio di attacchi informatici finalizzati allo spionaggio industriale.

In questo contesto, sempre la proposta del Digital Omnibus[21] di istituire un punto unico di segnalazione degli incidenti informatici ("*single-entry point for incident reporting*") rappresenterebbe un passo avanti contro tali minacce, razionalizzando gli obblighi di *reporting* oggi disciplinati da molteplici atti legislativi.

Parallelamente, la recente carenza di chip, conseguenza di una produzione di semiconduttori concentrata in un numero ristretto di paesi (soprattutto Taiwan, Corea del Sud e Stati Uniti), ha palesato una critica fragilità nella catena di approvvigionamento europea[22].

Un ulteriore ambito di importanza strategica è rappresentato dal settore spaziale. L'erogazione di servizi digitali europei dipende, infatti, dai servizi e dai dati forniti dai programmi Galileo, EGNOS e *Copernicus*. L'UE ha perseguito l'obiettivo di sviluppare una piena

---

[20] Con l'art. 1, paragrafi 3 e 4, che modifica gli artt. 4(8) e 5(11) del Data Act.

[21] Con gli articoli 6 e 9.

[22] Si veda la comunicazione della Commissione al Parlamento Europeo COM (2022) 45, p. 22. Secondo cui è necessario «*potenziare le capacità di leadership europea nel campo dei semiconduttori costituisce un prerequisito per la competitività futura, nonché una questione di sovranità tecnologica e sicurezza*».

autonomia in questo settore rispetto ai paesi terzi, con il programma Galileo che rappresenta la "prima infrastruttura pubblica di proprietà delle istituzioni europee"[23], seppur ancora, per il numero esiguo dei satelliti geostazionari orbitanti e quelli di previsto lancio "ad orbita bassa", non abbia raggiunto alcuna totale autosufficienza strategica in ambito securitario difensivo[24].

I dati e le tecnologie spaziali, infatti, possiedono un carattere *dual-use*, potendo essere impiegati tanto per scopi civili quanto per finalità di politica estera e di difesa, come dimostrato, nel corso del conflitto Russo-Ucraino, dalla costellazione di satelliti ad orbita bassa della compagnia privata statunitense *SpaceX* e dal connesso servizio internet di comunicazione satellitare *Starlink*, che ha consentito alle forze di Kiev di comunicare nonostante la rete internet del paese fosse stata pesantemente compromessa, fin dall'inizio, dalle forze d'invasione russe.

Il controllo autonomo di tali tecnologie non risponde, pertanto, alla sola esigenza di prosperità economica, ma investe direttamente la sicurezza nazionale e la resilienza collettiva.

Per tutto questo, l'analisi delle tecnologie critiche delinea i contorni di una sfida esistenziale per l'Unione Europea. La dipendenza strategica in settori chiave come i semiconduttori, le reti 5G e persino nello spazio, sebbene parzialmente mitigata da alcuni "tentativi" come il programma Galileo, rivela una vulnerabilità sistemica. Questa fragilità non è solo economica, ma si traduce direttamente in un deficit di sicurezza e sovranità, come dimostrato dalla crisi dei *microchip* e dai rischi di spionaggio legati alle infrastrutture di telecomunicazione.

Il quadro normativo, con il regolamento sul controllo degli investimenti esteri, rappresenta un primo, necessario tentativo di proteggere il tessuto produttivo e tecnologico europeo. Tuttavia, la mera protezione da interferenze estere si rivela una strategia difensiva e insufficiente. La constatazione del ritardo europeo e la natura *dual-use* di queste tecnologie pongono con urgenza la transizione da una posizione di difesa a una di leadership proattiva. Il passo successivo

[23] Si veda il comunicato finale della Commissione al Parlamento UE COM (2006) 272.

[24] ISPI, *Starlink e gli "altri": i (nuovi) pilastri della Terra*, 1 luglio 2025.

è trasformare la consapevolezza delle vulnerabilità in un progetto concreto di indipendenza produttiva e autonomia strategica.

È proprio da questa esigenza che scaturisce la necessità di esaminare il concetto di autonomia strategica tecnologica. Se le tecnologie critiche rappresentano lo strumentario a cui prestare attenzione, l'autonomia strategica ne costituisce il fine politico.

## 3. *L'obiettivo della sovranità tecnologica dell'UE*

Il perseguimento di un'autonomia strategica tecnologica rappresenta una priorità fondamentale per l'Unione Europea, in quanto presupposto indispensabile per garantire non solo la sua prosperità economica, ma anche la sua sicurezza e la sua capacità di agire indipendentemente sulla scena globale. Tuttavia, per comprendere appieno la portata di questo obiettivo strategico, è necessario inquadrarlo come la risposta operativa e dinamica al più ampio e fondante concetto di sovranità tecnologica. Se l'autonomia strategica designa il processo – l'insieme di politiche industriali, investimenti nella ricerca e strumenti di difesa commerciale volti a ridurre le dipendenze critiche – la sovranità tecnologica ne delinea lo status finale desiderato: la piena capacità dell'UE di autodeterminare il proprio futuro digitale, di definire valori e standard normativi e di controllare le infrastrutture critiche che sorreggono la sua società ed economia.

In questa prospettiva, la sovranità tecnologica costituisce l'obiettivo finale che orienta e giustifica l'intero progetto di autonomia strategica. Le tre dimensioni della sovranità – funzionale per lo sviluppo del mercato interno, per la protezione da minacce esterne e per l'affermazione di un modello normativo – forniscono la piattaforma concettuale su cui costruire un'autonomia concreta e resiliente[25].

Il concetto di "sovranità tecnologica" venga utilizzato dalle istituzioni europee per designare la capacità dell'Unione di impiegare la tecnologia digitale come strumento funzionale al corretto funziona-

[25] A. Barone, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law*, 2020, 1, p. 66.

mento del mercato interno. In questa accezione, che la rende semanticamente sovrapponibile a "sovranità digitale", la tecnologia non è fine a sé stessa, ma diviene l'infrastruttura abilitante per l'esercizio stesso di poteri sovrani in ambito economico e sociale[26].

La dipendenza ormai strutturale di servizi essenziali e attività economiche fondamentali – dall'energia alla sanità alla finanza – dalle tecnologie digitali trasforma la semplice competitività in una questione di resilienza sistemica e sopravvivenza del modello socio-economico europeo.

La stessa sovranità risulta, pertanto, compromessa dalla dipendenza tecnologica da attori extraeuropei, percepita non più come uno svantaggio concorrenziale, ma come una fonte di vulnerabilità strategica e un rischio sistemico. Il caso paradigmatico è rappresentato dalle infrastrutture 5G, definite "abilitatori chiave" per i servizi digitali, dove il ritardo tecnologico europeo e l'affidamento a fornitori soggetti a controllo statale straniero pongono seri interrogativi di sicurezza, esponendo gli Stati membri a rischi di spionaggio industriale e potenziale sabotaggio. Le istituzioni europee hanno mostrato piena consapevolezza di queste criticità, con il Parlamento UE che ha segnalato i pericoli di *backdoor*[27] nelle apparecchiature e la Commissione che ha sottolineato le gravissime conseguenze di eventuali interruzioni di reti divenute essenziali per servizi critici.

Le vulnerabilità si estendono ben oltre il settore delle telecomunicazioni, toccando in modo critico la produzione di semiconduttori – la cui concentrazione geografica ha rivelato la fragilità delle catene di approvvigionamento globali – e il settore spaziale. In quest'ultimo ambito, nonostante i significativi sforzi per costruire un'autonomia attraverso programmi come Galileo, EGNOS[28] e *Copernicus*, la dipendenza strategica non è stata completamente superata. La natura *dual-use* di queste tecnologie, utilizzabili tanto per scopi civili

[26] T. MADIEGA, *Digital Sovereignty for Europe*, PE 651.992, European Parliamentary Research Service, 2020.

[27] Ne è un esempio il caso, del dicembre 2021, delle telecamere di videosorveglianza, presso l'aeroporto di Fiumicino, della società Hikvision, controllata dall'azienda di stato cinese CETC.

[28] Acronimo di "European Geostationary Navigation Overlay Service" (satelliti UE).

che di difesa e *intelligence*, ne conferma la rilevanza diretta per la sicurezza collettiva e l'azione internazionale dell'Unione.

È proprio nel dominio della sicurezza che la sovranità tecnologica rivela la sua accezione più stringente. Viene invocata per affrontare minacce ibride e *cyber*, dove si afferma la necessità di possedere tecnologie autonome per proteggere le infrastrutture critiche e la sfera democratica, senza dipendere da paesi terzi per svolgere questo compito fondamentale di autotutela. La sicurezza nazionale, in questo contesto, diventa inscindibile dalla sicurezza tecnologica.

Un ulteriore pilastro strategico emerge con chiarezza dalla Comunicazione sulla strategia industriale europea, che opera una saldatura concettuale tra sovranità tecnologica e autonomia strategica. Il *focus* si sposta sul potenziamento della capacità industriale dell'UE nelle infrastrutture digitali critiche, riconoscendo che la resilienza e l'indipendenza si costruiscono attraverso una base produttiva e innovativa robusta e competitiva. Il Parlamento europeo ha ribadito con forza tale visione, sottolineando la necessità non solo di preservare, ma di sviluppare una *leadership* nelle tecnologie abilitanti fondamentali, intervenendo sulle intere catene del valore e sulla sicurezza di approvvigionamento dei materiali critici[29].

In questo sforzo, la semplificazione normativa proposta dal recente atto COM(2025) 837, giocherebbe un ruolo abilitante, riducendo i costi di *compliance* per le imprese, in particolare le PMI e le piccole *mid-cap*, e favorendo così gli investimenti in aree strategiche[30].

L'ambizione finale, tuttavia, non è solo meramente difensiva. Il raggiungimento di una posizione di *leadership* digitale a livello globale è visto come il veicolo per permettere all'UE di trasporre il suo peso normativo e i suoi valori nello scenario globale. In questa prospettiva, la sovranità tecnologica diventa la leva per esportare il "modello regolatorio europeo", trasformando l'Unione da arbitro a architetto dell'ordine digitale globale, e rafforzando in modo proattivo la propria autonomia strategica. Non a caso, il consolidamento

[29] Si veda la risoluzione del Parlamento UE del 25 novembre 2020.

[30] Il paragrafo 15 dell'art. 1, estende le esenzioni per PMI alle *small mid-cap companies*.

del quadro normativo digitale proposto dal "Digital Omnibus", con i paragrafi 27-58 dell'art. 1[31], presenterebbe un modello regolatorio europeo più coerente, solido e facilmente attuabile, spendibile per maggiore efficacia internazionale.

Sebbene i concetti di "sovranità tecnologica" e "sovranità digitale" vengano spesso utilizzati in modo sinonimico, può sussistere tra essi una gerarchia, dove la seconda è considerata prerequisito della prima. In sintesi, le invocazioni della sovranità tecnologica nella politica UE si articolano attorno a tre obiettivi principali e interdipendenti: garantire la continuità dei servizi essenziali nell'economia moderna (dimensione funzionale), potenziare la competitività globale dell'Unione (dimensione economica) e aumentare la resilienza verso attacchi ed ingerenze (dimensione securitaria). La proposta di futura regolazione "Digital Omnibus" interverrebbe sui tre aspetti: semplificando l'accesso e il riutilizzo dei dati del settore pubblico (funzionale), riducendo i costi per le imprese (economica) e razionalizzando la segnalazione degli incidenti informatici (securitaria)[32]. Una tale articolata e polifunzionale formulazione delineerebbe un concetto ampio e composito, che funge da cornice giustificativa per un vastissimo programma legislativo (dall'intelligenza artificiale alla governance dei dati, dalla connettività alla politica commerciale e industriale). La sua evoluzione semantica riflette la transizione dell'UE da un attore prevalentemente regolatorio a un attore strategico che cerca di affermare il proprio ruolo sistemico nell'arena tecnologica globale, rendendo la sovranità tecnologica una priorità politica assoluta per il futuro progetto europeo.

## 4. *Il quadro normativo di riferimento*

Il percorso giuridico verso l'autonomia strategica digitale dell'Unione Europea poggia su un fondamento primario: l'art.114 del TFUE. Questa disposizione, che permette di armonizzare le legislazioni nazionali per il funzionamento del mercato interno, è lo strumento cardine con cui l'UE disciplina i servizi digitali, agendo

[31] Che consolidano le misure del Data Act.

[32] Con l'art. 1 (intero), che modifica il *Data Act* e gli artt. 6 e 9 sui *single-entry point*; oltre all'Explanatory Memorandum, sulla riduzione oneri.

come potente motore di integrazione normativa. Tuttavia, la sfida della sovranità tecnologica, che mira a ridurre le pericolose dipendenze da paesi terzi, spinge l'azione dell'Unione ben al di là del mercato unico, verso territori giuridici più complessi.

Emerge, or dunque, una tensione costituzionale fondamentale. Da un lato, l'UE deve intervenire in settori cruciali come le reti 5G o lo Spazio, dove agisce in competenza concorrente con gli Stati membri; dall'altro, queste misure incidono inevitabilmente sul nucleo sensibile della sicurezza nazionale, che il Trattato riserva alla competenza esclusiva degli Stati. È il paradosso di un'autonomia strategica che, per essere realizzata, richiede all'Unione di addentrarsi in campi in cui i poteri tradizionali degli Stati membri sono più gelosamente custoditi[33].

Questa tensione si riproduce in politica industriale, dove gli obiettivi della Commissione si scontrano con una competenza UE limitata al solo coordinamento. Per colmare questa lacuna, l'Unione ricorre strategicamente a tutte le basi giuridiche disponibili, dal mercato interno allo sviluppo tecnologico. A dimostrazione di ciò, si consideri che per il settore spaziale l'art. 189 TFUE non impone un'autorità centralizzata, ma sancisce un modello di cooperazione che preserva un ruolo cruciale per gli Stati membri e per l'Agenzia Spaziale Europea, un compromesso che riflette la natura ibrida della governance europea.

È proprio in questo spazio di tensione che si colloca la risposta normativa alla minaccia cibernetica, incarnata dalle Direttive NIS[34]. Attuate in Italia, per la c.d. "NIS 2" con il D.Lgs. n. 123 del 2023, queste direttive, fondate proprio sull'art. 114 TFUE, dimostrano come l'armonizzazione del mercato interno sia la leva per costruire una sicurezza cibernetica comune. La proposta "Digital Omnibus" si inserirebbe in questo solco, intervenendo con l'art.6, proprio sulla direttiva NIS 2 (tra gli altri atti) per introdurre l'obbligo di utilizzare il punto unico di segnalazione, ottimizzando così l'architettura di sicurezza esistente. Tuttavia, questo quadro europeo deve

[33] S. Poli, E. Fahe, *The strengthening of the European Technological Sovereignty and its legal bases in the Treatie*, in *Rivista EuroJus.it*, fasc. n. 2/2022, p. 157.

[34] Rispettivamente Direttiva (UE) 2016/1148 (c.d. "NIS 1") e Direttiva (UE) 2022/2555 (c.d. "NIS 2").

coordinarsi con il perimetro di sicurezza nazionale cibernetica italiano e con i poteri del DIS[35], a testimonianza di un equilibrio continuo tra potestà europea e prerogative nazionali.

In definitiva, la ricerca di una base giuridica per la sovranità tecnologica costringe l'UE a navigare il delicato equilibrio tra il principio di attribuzione dei poteri e le esigenze imperative della sicurezza collettiva. Il paradosso finale è che il raggiungimento di un'autonomia strategica digitale, obiettivo fondamentale per la sopravvivenza dell'Europa come attore globale, potrebbe richiedere agli Stati membri di accettare una maggiore integrazione europea proprio in quelle aree – come la sicurezza – in cui hanno tradizionalmente difeso con più forza la propria sovranità.

Proprio partendo da questa complessa architettura di competenze, è necessario scendere nel dettaglio delle misure concrete attraverso cui l'Unione tenta di attuare la sua strategia per la sovranità tecnologica. Si può osservare come l'azione dell'UE si articoli in due direzioni complementari: una di natura preventiva, finalizzata a evitare un ulteriore erosione della base tecnologica europea, e una di carattere reattivo e costruttivo, che mira a colmare attivamente le dipendenze strategiche esistenti.

Sul versante preventivo, lo strumento cardine è il Regolamento (UE) 2019/452, che istituisce un quadro per il controllo degli investimenti diretti esteri. Fondato sulla politica commerciale comune, un'area di competenza esclusiva dell'Unione, questo atto rappresenta un meccanismo di "*screening*" che autorizza gli Stati membri a valutare le operazioni di investimento straniero che potrebbero minacciare l'ordine pubblico o la sicurezza, con particolare attenzione alle infrastrutture e tecnologie critiche. In questo sistema ibrido, la Commissione svolge un ruolo cruciale di monitoraggio e coordinamento, potendo emettere pareri vincolanti nel caso in cui un investimento abbia ripercussioni transnazionali[36]. Tuttavia, è importante sottolineare la natura intrinsecamente difensiva di questo strumento: esso funge da argine contro un ulteriore peggioramento della dipendenza tecnologica, ma non possiede la capacità intrin-

[35] Dipartimento delle Informazioni per la Sicurezza della Repubblica Italiana.

[36] L. CALIFANO, *La strategia normativa dell'Unione europea per un nuovo ordine digitale*, in *federalismi.it*, n. 15/2025.

seca di costruire alternative europee o di rimediare alle vulnerabilità strutturali già esistenti.

È dunque sul versante reattivo e costruttivo che si gioca la partita più significativa, e al contempo, più problematica dal punto di vista giuridico. Le misure che rientrano in questa categoria sono le più ambiziose, poiché mirano a costruire *ex novo* la capacità industriale e tecnologica dell'Unione. È proprio in questo ambito che emerge con forza la questione dell'appropriatezza della base giuridica. Queste iniziative spingono spesso ai limiti le competenze europea, testando la flessibilità dei Trattati.

La recentissima proposta COM(2025) n.837 rappresenta un esempio emblematico di questo approccio costruttivo. Pur fondandosi sull'art. 114 TFUE, ha come scopo[37] non è solo armonizzare il mercato, ma potenziare la competitività e la resilienza tecnologica europea attraverso una regolazione più efficace.

Un primo gruppo di misure, che sarà analizzato in dettaglio, opera in settori dove l'UE dispone di quelle che potremmo definire competenze "deboli" o *soft*[38], come il coordinamento in materia industriale o il sostegno alla ricerca. Qui, l'Unione deve ricorrere a un'ingegneria giuridica sofisticata, spesso combinando diverse basi giuridiche e promuovendo una cooperazione intergovernativa rafforzata, come nel caso dei progetti di comune interesse europeo (IPCEI).

Un secondo gruppo, invece, trova il suo fondamento più solido nell'art. 114 TFUE, sfruttando la logica del mercato interno per legittimare interventi che hanno chiare finalità strategiche e securitarie. Atti come il *Data Governance Act* o il *Digital Markets Act* rientrano in questa categoria, dimostrando come l'obiettivo dell'armonizzazione normativa possa essere funzionalizzato alla costruzione di un'arena digitale più equa, sicura e favorevole all'emergere di campioni industriali europei[39].

---

[37] Si vedano i consideranda 1 e 7.

[38] De Gregorio; O. Pollicino; P. Dunn, *Digitisation and the central role of intermediaries in a post-pandemic world*, in *Medialaws.eu*, 2021.

[39] M. Orofino, *Il Digital Market Act*, in *La regolazione europea della società digitale* (a cura di) F. Pizzetti; S. Calzolaio; A. Iannuzzi; E. Longo; M. Orofino, Torino, 2024, p. 182 e ss.

L'utilizzo di questa base giuridica, sebbene potenzialmente controverso quando l'obiettivo primario è strategico piuttosto che meramente *market-making*, rappresenta uno degli espedienti più potenti a disposizione delle istituzioni per avanzare l'agenda della sovranità tecnologica entro i confini, pur elastici, dell'attuale quadro costituzionale dell'Unione.

## 5. *Approcci alla regolazione delle nuove tecnologie critiche per la sicurezza cibernetica UE*

L'Unione Europea, parallelamente alla regolazione e allo sviluppo del mercato digitale, sta sviluppando un articolato ecosistema istituzionale e normativo per rafforzare le proprie capacità nel dominio delle tecnologie critiche, con particolare riferimento alla sicurezza cibernetica. Accanto agli strumenti di vigilanza sugli investimenti esteri, l'architettura di sicurezza europea si sta arricchendo di nuove strutture operative e di coordinamento.

Particolarmente significativa è l'istituzione del Centro europeo di competenza per la cibersicurezza e della corrispondente rete dei centri di coordinamento nazionali, insieme al potenziamento dell'Istituto europeo di innovazione e tecnologia[40].

Queste iniziative, fondate sugli artt. 173(3) e 188(1) TFUE, mirano a sviluppare le capacità tecnologiche, industriali e di ricerca dell'Unione nel settore della cibersicurezza, aumentandone complessivamente la competitività strategica[41].

Parallelamente, la Commissione ha proposto l'adozione di un Regolamento basato sugli articoli 185 e 187 TFUE che istituisce imprese comuni, tra cui l'Impresa comune per le reti e i servizi intelligenti. Questo partenariato strategico sostiene la sovranità tecnologica in linea con la nuova Strategia industriale per l'Europa e lo strumentario per la cibersicurezza 5G, contribuendo alla risoluzione di sfide societarie e alla transizione digitale e verde.

In questo contesto, il futuro regolamento "Digital Omnibus" attribuirebbe all'ENISA (l'Agenzia dell'UE per la cibersicurezza) il compito di sviluppare e gestire il punto unico di segnalazione degli

[40] Vd. Regolamento (EU) 2021/819.

[41] Si veda il Rapporto sull'Indipendenza Digitale in Italia - Redopen (2024).

incidenti, potenziando così il ruolo operativo di un'agenzia europea già chiave nel settore[42].

Il programma spaziale europeo: un caso paradigmatico di competenza condivisa.

Un ulteriore sviluppo legislativo di rilievo riguarda l'istituzione e la gestione del programma spaziale dell'UE e della corrispondente Agenzia del programma spaziale europea nel 2021[43]. La tecnologia spaziale rappresenta infatti un'infrastruttura critica essenziale non solo per il funzionamento del mercato interno, ma anche per servizi fondamentali delle economie moderne e per la sicurezza interna ed esterna dell'Unione, materia che in linea di principio rientra nella competenza esclusiva degli Stati membri.

Il programma spaziale, invece, si propone di fornire o contribuire a fornire servizi, informazioni e dati spaziali aggiornati, di alta qualità e, ove appropriato, sicuri per sostenere le priorità politiche dell'Unione. Significativamente, tra i suoi obiettivi dichiarati vi è il rafforzamento della sicurezza intrinseca ed estrinseca dell'Unione e dei suoi Stati membri e il potenziamento dell'autonomia dell'Unione, in particolare in termini di tecnologia[44].

L'evoluzione verso una governance integrata della sicurezza spaziale è ulteriormente confermata dall'adozione di una decisione PESC che attribuisce all'Alto rappresentante responsabilità specifiche nella prevenzione delle minacce spaziali, includendo persino la facoltà di emanare "istruzioni provvisorie" all'Agenzia in caso di emergenza. Questo assetto normativo segna una progressiva assunzione di funzioni di sicurezza spaziale a livello UE, tradizionalmente riservate alla sovranità nazionale.

Tra le misure volte a rafforzare la sovranità tecnologica europea, quelle basate sull'art. 114 TFUE sollevano, inoltre, particolari questioni di legittimità costituzionale. Questa disposizione, conce-

---

[42] Art. 6, paragrafo 1.

[43] Vd. Regolamento (UE) 2021/696 del Parlamento UE e del Consiglio, del 28 aprile 2021, che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale e abroga i regolamenti (UE) n. 912/2010, (UE) n. 1285/2013 e (UE) n. 377/2014 e la decisione n. 541/2014/UE, GU [2021], L 170/69.

[44] R. Hansen, *Towards a EU Industrial Policy for the Space Sector*, in T. Hörber; P. Stephenson (a cura di), *European Space Policy. European Integration and the Final Frontier*, Londra, 2015, pp. 224-238.

pita per il ravvicinamento delle legislazioni nazionali finalizzato al funzionamento del mercato interno, viene progressivamente estesa a settori che lambiscono la sicurezza nazionale.

Si osserva infatti una tendenza a utilizzare l'art. 114 TFUE oltre i limiti consentiti dal principio di attribuzione delle competenze[45], configurando quella che potrebbe definirsi una progressiva "mercificazione della sicurezza dell'UE". Questo approccio rischia di implicare una significativa erosione delle competenze tradizionali degli Stati membri nel campo della sicurezza, nonostante il chiaro dettato dell'art. 4 (par. 2) TUE che riconosce la sicurezza nazionale come competenza essenziale degli Stati.

La proposta del "Digital Omnibus", che modificherebbe atti come la direttiva NIS 2 e il regolamento DORA[46] per introdurre l'obbligo di reporting unificato, si colloca proprio in questo solco, utilizzando la base giuridica del mercato interno per armonizzare e potenziare un aspetto cruciale della sicurezza cibernetica.

La Corte di giustizia dell'UE (CGUE) , in particolare nel celebre giurisprudenza "*Digital Rights Ireland*"[47] che ha annullato la direttiva sulla conservazione dei dati, dimostra la tensione tra l'utilizzo dell'art. 114 TFUE e la tutela dei diritti fondamentali. Tuttavia, rimane ancora limitata la giurisprudenza specifica sull'uso di questa base giuridica per misure di sicurezza in senso stretto.

Tuttavia, l'utilizzo sistematico dell'art. 114 TFUE per misure che perseguono primariamente obiettivi di sicurezza appare spingere ai limiti l'interpretazione giurisprudenziale della Corte di giustizia, secondo cui la scelta della base giuridica deve basarsi su «*elementi obiettivi, tali da poter formare oggetto di controllo giurisdizionale, in particolare lo scopo e il contenuto dell'atto*»[48]. In diversi casi

---

[45] S. Weatherill, *The competence to harmonise and its limits* in P. Koutrakos; J. Snell, *Research Handbook on the Law of the EU's Internal Market*, Chelthenam/ Northampton, 2017, p. 82 ff.

[46] Art. 6 (NIS2) e art. 8 (DORA), modifica gli atti per il reporting unificato.

[47] Precisamente le pronounce della Corte di Giustizia dell'Unione Europea C-293/12 and C-594/12 *Digital Rights Ireland Ltd vs Minister for Communications, Marine and Natural Resources and Others e Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

[48] Delineato nella pronuncia CGUE sul caso C-376/98, *Germany vs Council*, ECLI:EU:C:2000:544.

esaminati, non appare effettivamente e oggettivamente evidente che lo scopo primario degli atti sia migliorare le condizioni di instaurazione e funzionamento del mercato interno[49], configurando così una potenziale violazione del principio di attribuzione delle competenze.

Da tutto questo, quindi, si evince come l'Unione Europea stia progressivamente costruendo un complesso ecosistema normativo e istituzionale per la sicurezza cibernetica, muovendosi lungo un duplice binario. Da un lato, attraverso il potenziamento di centri di competenza e partenariati industriali fondati su basi giuridiche "deboli", dall'altro mediante un'estensione sempre più spinta dell'art. 114 TFUE a settori liminari della sicurezza nazionale. Il futuro "Digital Omnibus", rappresenterebbe questa duplice strategia: da un lato semplifica e consolida la regolazione di mercato, dall'altro, attraverso misure come il punto unico di segnalazione, avanza un'agenda di sicurezza integrata[50]. Questo approccio ibrido riflette la tensione irrisolta tra l'esigenza di preservare le competenze sovrane degli Stati membri e l'imperativo strategico di dotare l'Unione degli strumenti necessari per affrontare le nuove minacce tecnologiche[51].

Tale tensione si inserisce in una sfida geopolitica più ampia: la necessità di contrapporre allo strapotere delle Big Tech americane e alla crescente penetrazione delle tecnologie cinesi un autentico modello digitale europeo. Le iniziative analizzate – dal Centro per la cibersicurezza al programma spaziale, fino alle diverse direttive sulla resilienza digitale – rappresentano altrettanti tasselli di una strategia volta a costruire una "terza via" europea nell'arena tecnologica globale. Una via che cerchi di coniugare l'innovazione con la tutela dei diritti fondamentali, la sicurezza con i valori democratici, la competitività con la sovranità tecnologica.

Tuttavia, la stessa ambizione di creare un mercato digitale europeo competitivo e autonomo si scontra con i limiti strutturali del sistema dei Trattati. L'utilizzo "creativo" dell'art. 114 TFUE, seb-

---

[49] Si vedano i casi giurisprudenziali C-270/12, *UK vs Parliament/Council*, ECLI:EU:C:2014:18, par. 113 e C-66/04, *UK vs Parliament and Council*, ECLI:EU:C:2005:743, par. 44.

[50] Art. 1 (consolidamento) e artt. 6-9 (sicurezza).

[51] L. Previti, *Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *federalismi.it*, n. 25/2022.

bene funzionale a superare le rigidità del principio di attribuzione, rischia di minare la legittimità costituzionale dell'intera architettura di sicurezza digitale dell'UE. Il paradosso è che proprio la necessità di proteggere il mercato unico dalla dipendenza tecnologica esterna spinge l'Unione verso un'espansione funzionale delle proprie competenze che potrebbe alterare gli equilibri fondamentali dell'assetto istituzionale europeo.

La sfida che attende l'UE nei prossimi anni sarà dunque duplice: da un lato, sviluppare capacità tecnologiche autonome in grado di competere con i colossi extraeuropei senza rinunciare al proprio modello di società; dall'altro, trovare un nuovo equilibrio costituzionale che, nel rispetto del principio di attribuzione, consenta all'UE di agire efficacemente come attore strategico nella competizione tecnologica globale. Solo risolvendo tale problematico binomio l'Europa dei 27 potrà trasformare la sua vulnerabilità in una leva di sovranità e influenza mondiale.

## 6. *Conclusioni*

Il complesso rapporto tra Big Tech, tecnologie critiche e autonomia strategica dell'Unione Europea delinea un panorama articolato e dinamico, che chiama in causa il futuro stesso del progetto europeo. La sfida tecnologica si rivela, in ultima istanza, una sfida esistenziale che investe simultaneamente la sicurezza collettiva, la prosperità economica e la capacità dell'UE di preservare il suo modello di società fondato sui valori democratici.

Ci troviamo di fronte a una transizione cruciale, in cui il soggetto Unione Europea intende passare, da mero "consumatore ideale" di tecnologie digitali a potenziale attore globale nella competizione tecnologica. Questo passaggio, reso necessario dalla dipendenza strategica da attori extraeuropei e dall'oligopolio delle Big Tech, richiede un ripensamento profondo delle categorie giuridiche e politiche tradizionali.

La distinzione tra sicurezza nazionale e regolazione del mercato si fa sempre più labile, mentre emergono nuove forme di potere ibrido esercitato da attori privati transnazionali il cui impatto sulle società europee spesso sorpassa quello di molti Stati sovrani.

In questo contesto, il programma di rafforzamento della Politica di Sicurezza e Difesa Comune (PSDC) e il Piano UE *Readiness* 2030 rappresentano componenti essenziali di questa trasformazione e volontà dell'UE di investire maggiormente sulle tecnologie critiche digitali, tanto in termini di autonomia e concorrenza commerciale, quanto in ottica strategica difensiva.

Tuttavia, la loro efficacia sarà determinata dalla capacità di integrare organicamente la dimensione tecnologica con quelle tradizionali della difesa e della sicurezza.

La dipendenza dall'industria bellica statunitense e dai suoi ecosistemi tecnologici costituisce un paradosso strategico che il *Readiness 2030* dovrà risolvere (seppur in un primo periodo non potrà fare a meno delle forniture statunitensi e britanniche): come potenziare le capacità difensive europee senza perpetuare una vulnerabilità tecnologica che ne mina alla base l'autonomia decisionale?

La risposta risiede in un approccio olistico che consideri la natura *dual-use* delle tecnologie critiche come elemento centrale della sicurezza collettiva, l'interdipendenza tra resilienza digitale e capacità difensive nell'era della guerra ibrida, e la necessità di sviluppare una base industriale europea in settori strategici come i semiconduttori, l'intelligenza artificiale e le reti di telecomunicazione di nuova generazione.

In questo sforzo, la semplificazione normativa prospettata con la proposta "Digital Omnibus" non è un mero esercizio tecnico ma un moltiplicatore di forza[52].

L'analisi del quadro normativo evidenzia una tensione costitutiva tra l'esigenza di un'azione europea efficace e il rispetto del principio di attribuzione delle competenze.

L'utilizzo strumentale dell'art. 114 TFUE, sebbene funzionale a superare le rigidità dei Trattati, solleva questioni di legittimità costituzionale che non possono essere eluse. La progressiva "mercificazione della sicurezza" attraverso l'estensione della logica del mercato interno a settori sensibili rischia di alterare gli equilibri fondamentali dell'assetto istituzionale europeo.

---

[52] Vdd. *Explanatory Memorandum* (pagine 3-4).

Tuttavia, questa tensione potrebbe risolversi in un nuovo equilibrio costituzionale che, nel rispetto dei valori fondanti dell'Unione, consenta una governance più integrata delle sfide tecnologiche e securitarie. La stessa necessità di proteggere il mercato unico dalla dipendenza tecnologica esterna potrebbe spingere gli Stati membri ad accettare un trasferimento di sovranità funzionale in ambiti tradizionalmente considerati di competenza nazionale.

La sfida che attende l'Unione nei prossimi anni sarà dunque duplice: sviluppare capacità tecnologiche autonome in grado di competere con i colossi extraeuropei senza rinunciare al proprio modello di società, e al contempo trovare un nuovo equilibrio istituzionale che consenta all'UE di agire efficacemente come attore strategico nella competizione tecnologica globale.

Le misure adottate (dal Centro europeo di competenza per la cibersicurezza al programma spaziale, alle direttive NIS, fino al regolamento sugli investimenti esteri) rappresentano altrettanti tasselli di una strategia complessiva volta a costruire quella "terza via" europea nell'arena tecnologica globale che cerchi di coniugare l'innovazione con la tutela dei diritti fondamentali, la sicurezza con i valori democratici, la competitività con la sovranità tecnologica. Il successo di questo ambizioso progetto dipenderà dalla capacità dell'Unione di tradurre la sua vulnerabilità digitale in una leva di influenza mondiale, trasformando la consapevolezza dei rischi in una visione strategica in grado di guidare; tanto l'azione normativa quanto lo sviluppo industriale e la cooperazione internazionale.

In questo senso, la sovranità tecnologica non rappresenta solo una questione di sicurezza o di prosperità economica, ma si configura come il presupposto necessario per la sopravvivenza stessa dell'Europa come attore globale e come comunità di valori comuni. L'autonomia strategica tecnologica, pertanto, non è un sogno velleitario, ma un cantiere giuridico, industriale e costituzionale aperto, i cui esiti definiranno la sovranità europea nel XXI secolo[53].

[53] Il contributo è stato realizzato dall'Autore nel corso delle ricerche per il progetto di ricerca nazionale PNRR "Security and Rights in CyberSpace" – SERICS (ACK: PE00000014).

ANTONIO FOTI

# LA CO-REGOLAZIONE NELL'AI ACT: LA SFERA DI HOBERMAN

SOMMARIO: 1. Introduzione. – 2. La co-regolazione a maglie larghe nel GDPR. – 3. La co-regolazione a maglie strette nel Digital Package. – 4. La co-regolazione nell'AI Act. – 5. La co-regolazione nell'AI Act, assimilabile a una sfera di Hoberman. – 6. Osservazioni conclusive.

## 1. *Introduzione*

Il presente contributo analizza lo strumento della co-regolazione all'interno della società digitale[1].

La regolazione della società digitale, come noto, presenta caratteristiche peculiari e innovative[2]. In primo luogo, essa si colloca in una dimensione globale: da un lato, deve garantire la libera circolazione dei dati nello spazio digitale, per antonomasia interconnesso e globale, in linea con la logica del *world wide web*; dall'altro,

[1] In dottrina si è molto discusso in merito allo strumento della co-regolazione nell'ambito delle nuove tecnologie digitali. A proposito, si veda F. PIZZETTI *et al.*, *La regolazione europea della società digitale*, Giappichelli, Torino, 2024; ID., *La regolazione europea dell'intelligenza artificiale nella società digitale*, Giappichelli, Torino, 2025. Ancora, si veda G. DE MINICO, *Internet. Regola e anarchia*, Jovene, Napoli, 2012; A. SIMONCINI, *La co-regolazione delle piattaforme digitali*, in *Riv. trim. di dir. pub.*, 2022, pp. 1031-1049; G. MOBILIO, *La co-regolazione delle nuove tecnologie tra rischi e tutela dei diritti fondamentali*, in *Osservatorio sulle fonti*, 1, 2024, pp. 245-270; G. DI COSIMO, *La co-regolazione delle tecnologie digitali: il paradigma centro-periferia*, in *Osservatorio sulle fonti*, 1, 2024; O. POLLICINO, *La regolazione digitale nell'Unione europea*, in *Riv. trim. dir. pubb.*, 4, 2022.

[2] Cfr. R. BROWNSWORD, E. SCOTTFORD, K. YEUNG, *The Oxford Handbook of Law, Regulation and Tecnology*, OUP, Oxford, 2017; R. BALDWIN, M. CAVE, *Understanding regulation. Theory, Strategy and Practice* (a cura di), OUP, Oxford, 2011; ID., *The Oxford Handbook of Regulation*, OUP, Oxford, 2013.

deve fronteggiare l'ascesa di grandi poteri privati, dotati di una capacità d'incidenza economica e sociale tale da influenzare l'esercizio dei diritti fondamentali e i processi democratici[3].

In secondo luogo, la società digitale si configura come una «società a cambiamento rapidissimo»[4], che richiede regole tecniche e un elevato livello di expertise, in grado di adattarsi all'innovazione senza soffocarla.

Tali caratteristiche sono cruciali per cogliere l'essenza della co-regolazione nella società digitale. La Commissione europea definisce la co-regolazione come «*un meccanismo con il quale l'Unione affida il raggiungimento di obiettivi politici specifici stabiliti dalla legislazione o da altri documenti, a parti privati riconosciute nel settore, in modo da combinare i vantaggi della natura vincolante della legislazione con l'approccio flessibile della autoregolazione*»[5].

Tale approccio risponde alla funzione classica della regolazione dei mercati, volta a promuovere lo sviluppo economico e la libera concorrenza[6]. Tuttavia, la società digitale ne trasforma la portata: la

---

[3] Cfr. P. Ciarlo, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, 2, 2018; O. Pollicino, *Potere digitale*, in *Enc. del dir.*, *I Tematici V*, 2023, pp. 410-446; G. Resta, *Poteri privati e regolazione*, in *Enc. del dir.*, *I Tematici V*, 2023.

[4] Come è stato opportunamente rilevato: «*Le tecnologie si sviluppano con una rapidità inaudita; le relazioni fra gli uomini e i popoli hanno una dimensione globale e una latitudine in cui, senza la mediazione della tecnica, l'orizzonte non è più visibile allo sguardo dell'uomo; il bisogno di comunicare, di raggiungere tutti e ognuno, convive con l'aspirazione ad un'esistenza sicura, posta al riparo da vecchi e nuovi pericoli. La società della tecnica, già diventata nel secolo scorso una società "a cambiamento veloce", è divenuta oggi una società "a cambiamento velocissimo"*». GPDP, *Discorso del Presidente Francesco Pizzetti* - Relazione 2005 - 7 luglio 2006.

[5] Commissione europea, *Better Regulation Tool-box*, edizione giugno 2023, cit., p. 124.

[6] La regolazione economica per antonomasia risponde all'esigenza di correggere i «fallimenti di mercato» con strumenti di tipo autoritativo. Cionondimeno si è assistito nl corso del tempo ad una evoluzione dei sistemi regolatori, condizionati dagli eventi e dalle diverse correnti ideologiche che hanno interessato il settore. Per un'analisi attenta di queste trasformazioni si rinvia a M. Clarich, *Alle radici del paradigma dei mercati*, in *Rivista della Regolazione dei mercati*, 2, 2020, pp. 230-239. Ancora, si veda il contributo fornito da G. Majone, *The traformations of regulatory State*, in *Osservatorio sull'Analisi d'Impatto della Regolazione*, 2010; M. Ramajoli, *Self regulation, soft regulation e hard regulation nei mercati finanziari*, in *Rivista della Regolazione dei mercati*, 2, 2016.

regolazione non è più rivolta soltanto all'equilibrio di mercato, ma anche – e soprattutto – alla tutela effettiva dei diritti fondamentali. Tale aspetto emerge in tutta la sua chiarezza nella regolazione dell'Intelligenza artificiale (AI)[7].

Le tecnologie di AI, già oggi, si mostrano come un formidabile alleato per il pieno godimento di diritti fondamentali: basti pensare all'ambito sanitario, in cui l'uso dell'AI garantisce diagnosi più veloci e precise rispetto a quelle umane e tecniche mediche innovative[8], aumentando la portata del diritto alla salute, *ex* art. 32 Cost.; oppure, si pensi al miglioramento, in termini di efficienza, della P.A. grazie all'utilizzo dell'AI[9], in linea con il principio di buon andamento dei pubblici uffici ai sensi dell'art. 97 Cost.

Di conseguenza, non solo un uso distorto dell'intelligenza artificiale può ledere i diritti degli individui, ma anche una regolamentazione eccessivamente restrittiva, volta a frenare l'innovazione, rischia di compromettere, in futuro, la portata e l'effettivo esercizio dei diritti fondamentali garantiti sia dalle Carte costituzionali degli Stati membri sia dalla Carta dei diritti fondamentali dell'Unione Europea[10].

---

[7] Sul punto si rinvia a A. D'Aloia, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Review*, 1, 2019, pp. 3-31. Ancora, G. De Minico, *Le fonti del diritto: un argine all'intelligenza artificiale?*, in *Rivista AIC*, 3, 2025, pp. 76-100; G. Sartor, *Intelligenza artificiale e diritto*, Giappichelli, Torino, 2022; M. D'Amico, *Costituzione, diritti, algoritmi: le sfide future per non perdere la bussola del costituzionalismo*, in F. Balanguer Callejòn, *La constitucion del algoritmo: recensiones, presentaciones y entrevistas* (coord.), Fundaciòn Manuel Giménez Abad, 2025, pp. 157-169.

[8] Sul punto si rinvia a E. Borgonovi, G. Migliore, *Digitalizzazione della sanità o sanità digitale?*, in *MECOSAN*, XXXI, 123, Franco Angeli Editore, Milano, 2020.

[9] In merito, si rinvia D. Galetta, J.G. Corvalàn, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *Federalismi.it*, 3, 2019; Ancora, A. Simonicini, *Profili costituzionali dell'amministrazione algoritmica*, in *Riv. trim. dir. pub.*, 4, 2019. Sul punto è intervenuta, inoltre, una rilevante pronuncia del Consiglio di Stato (Cons. St., sent. 8 aprile 2019, n. 2270) che, pur affermando come l'impiego di un algoritmo in una procedura concorsuale per l'assunzione di docenti debba conformarsi ai principi di imparzialità, pubblicità e trasparenza, ha al contempo riconosciuto la legittimità e l'utilità dell'utilizzo di sistemi di intelligenza artificiale nella Pubblica Amministrazione, in coerenza con l'esigenza di efficienza sancita dall'art. 97 Cost.

[10] Tale aspetto è stato opportunamente rilevato da M. Orofino, *One Digital*

Alla luce di ciò, ne consegue che la regolazione europea deve conciliare due esigenze diverse ma complementari: da un lato, garantire la protezione dei diritti fondamentali dell'individuo in relazione con le nuove tecnologie, dall'altro non ostacolare l'innovazione digitale, non solo in ottica del progresso economico-sociale, ma anche per aumentare la portata di tali diritti nel futuro. In tale ottica, l'Unione europea ha attribuito alla co-regolazione un ruolo di rilievo, seppur declinandolo in forme differenti nel corso del tempo.

Dal punto di vista metodologico, l'analisi che segue si fonda su un approccio diacronico e giuridico-sistematico, basato sull'esame dei principali strumenti normativi europei in materia digitale e dei relativi codici di condotta, con l'obiettivo di ricostruire l'evoluzione del modello di co-regolazione nel diritto dell'Unione. Per cogliere questa evoluzione della co-regolazione nella società digitale, essa verrà rappresentata come una rete a maglie, nella quale i nodi corrispondono al potere normativo pubblico, mentre la distanza che li separa esprime lo spazio e le modalità di intervento riconosciute agli attori privati nel processo regolativo. Tale allegoria consentirà di cogliere con chiarezza la natura relazionale della co-regolazione digitale, fondata su un intreccio costante di competenze e su un'interdipendenza strutturale tra pubblico e privato.

In tale prospettiva, come si cercherà di chiarire lungo questo contributo, è possibile individuare almeno due diverse fasi della co-regolazione all'interno della società digitale. Nella prima fase, segnata dall'approvazione del GDPR, emerge una *co-regolazione a maglie larghe*, laddove l'attore pubblico si limita a definire il quadro normativo generale, entro cui l'attore privato può legittimamente operare, tracciando in maniera chiara le rispettive sfere di competenza.

Nella seconda fase, caratterizzata dall'entrata in vigore del *Digital Package*, si assiste, invece, ad una *co-regolazione a maglie strette*, laddove il ruolo assunto dal regolatore europeo assume un carattere più stringente e penetrante: l'attore pubblico non si limita a fissare le condizioni di base, ma esercita un ruolo proattivo e

---

*Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti Supreme e Salute*, 1, 2025, pp. 1-19.

orientativo nel governo dell'innovazione digitale, incidendo in maniera più diretta sulle modalità di attuazione da parte dei privati.

Alla luce di ciò, la tesi che si cercherà di presentare in questo contributo è l'individuazione di una nuova evoluzione della co-regolazione, la quale assume una forma ibrida: il ruolo dell'attore pubblico è centrale ma, al tempo stesso, è coadiuvato nella stesura degli stessi obblighi dall'attore privato. Si prospetta, in altri termini, un approccio «multi-attoriale» della regolazione, volto al coinvolgimento «dei diversi soggetti che rivestono un ruolo cruciale nel funzionamento della tecnologia»[11].

Tale modello può essere efficacemente descritto attraverso la metafora della *sfera di Hoberman*: una struttura reticolare e adattiva, i cui nodi si espandono o si contraggono in funzione delle esigenze di tutela e di innovazione.

Nei paragrafi che seguono si analizzerà tale evoluzione, evidenziando, in particolar modo, le implicazioni del modello ibrido di co-regolazione – presente nell'AI Act – per l'equilibrio tra innovazione tecnologica e tutela dei diritti fondamentali nell'ordinamento europeo.

## 2. *La co-regolazione a maglie larghe nel GDPR*

Come noto, l'approvazione del Regolamento Generale sulla Protezione dei Dati Personali (GDPR)[12] ha rappresentato un cambio decisivo nella strategia di regolazione adottata dall'attore pubblico europeo.

Anzitutto, il GDPR si distanzia dall'approccio precedente (basato sulla Direttiva 95/46/CE) il quale poneva in rilievo il consenso dell'interessato, favorendo, invece, le ulteriori basi legali per il trattamento dei dati personali[13]. A questa estensione della base legale,

---

[11] A. Pajno *et al.*, *AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal*, 3, 2019, cit., p. 209.

[12] Reg. (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 (regolamento generale sulla protezione dei dati).

[13] In particolare, l'art. 6 GDPR prescrive che il trattamento è lecito, non solo quando l'interessato ha espresso il consenso al trattamento dei propri dati personali,

corrisponde una lunga lista di diritti dell'interessato[14] e l'elaborazione di obblighi in capo al titolare e al responsabile del trattamento[15]. Tali obblighi aumentano all'aumentare del rischio per i singoli individui, seguendo la logica della regolazione *risk-based*, in cui gli obblighi in capo al soggetto privato aumentano a seconda del diverso grado di rischio per i singoli e per la collettività[16].

Il GDPR incentra tutta la sua valenza trasformativa nel concetto di *accountability* di titolari e responsabili, ossia, «*sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento*»[17].

In altri termini, ai titolari è affidato il compito di determinare autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel pieno rispetto delle disposizioni normative e alla luce di specifici criteri indicati dal regolamento. Di conseguenza, l'intervento delle autorità di controllo assume prevalente-

---

ma anche quando sia necessario alla conclusione di un contratto (lett. *b*), per adempiere ad un obbligo legale (lett. *c*), per la salvaguardia di un interesse vitale dell'interessato o di altra persona fisica (lett. *d*), per l'esecuzione di un compito di pubblico interesse (lett. *e*), per legittimo interesse del titolare del trattamento (lett. *f*). Come si nota, si estendono le possibilità di trattamento di dati personali, in quanto il consenso è solo uno dei parametri di liceità.

[14] Tali diritti dell'interessato – elencati al Capo III, GDPR – sono la trasparenza del trattamento, l'informativa, il diritto di accesso, di rettifica, di cancellazione, di limitazione del trattamento e altri.

[15] Il Capo IV, sez. 1, GDPR elenca gli obblighi generali del titolare e del responsabile del trattamento di dati personali. La sez. 2 riguarda le misure tecniche e organizzate da mettere in atto, mentre la sez. 3 è dedicata alla valutazione d'impatto.

[16] Il *rischio digitale* può essere definito come una specificazione del più generale *rischio tecnologico*, ovvero una sua maggiore pervasività, in quanto, con la rivoluzione digitale, la tecnica diventa ancora più diffusa ed endemica rispetto a prima. In dottrina si è molto discusso sul concetto di regolazione del rischio in ambito digitale. Sul punto si rinvia a G. Giannone Codiglione, *Risk-based approach e trattamento dei dati personali*, in S. Sice, V. D'Antonio, G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Wolters Kluver-Cedam, Milano, 2016, p. 55 ss.; Ancora, si vedano A. Mantelero, *La gestione del rischio*, in G. Finocchiaro, *La protezione dei dati personali in Italia* (a cura di), Zanichelli, Bologna, 2019, p. 473 ss.; E. Longo, *La disciplina del rischio digitale*, in F. Pizzetti *et al.*, *op. cit.*, pp. 53-81.

[17] Così, GPDP, *Accountability (responsabilizzazione)*, consultabile al link: *https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili*. Cfr. GDPR, art. 24, cons. 74 e 78.

mente una funzione *ex post*, intervenendo cioè successivamente alle decisioni adottate autonomamente dal titolare.

Il GDPR, così, configura un regime di co-regolazione in cui il titolare del trattamento è libero di auto-regolarsi entro i confini, però, di una cornice di precetti normativi concepiti dal potere pubblico, volti a garantire il corretto concorso tra tutela dei dati personali e libera circolazione dei dati stessi. Si prospetta, in altri termini, una forma di co-regolazione che «*sprona i destinatari delle norme a scegliere le soluzioni organizzative e di governance più adatte per affrontare e gestire i rischi, sotto il controllo delle autorità pubbliche regolatrici che verificano se gli obiettivi prefissi dalla normativa sono stati raggiunti*»[18].

In questo senso, emerge il sistema di co-regolazione flessibile, definita a *maglie larghe*: il ruolo assunto dagli attori privati (titolari del trattamento) è volto alla definizione delle regole operative, mentre l'autorità pubblica esercita una funzione di controllo, più che di diretta conformazione delle condotte.

Tale approccio flessibile della co-regolazione emerge, finanche, nell'adozione dei codici di condotta. Gli artt. 40 e 41 del GDPR prevedono l'istaurazione di un dialogo tra attore pubblico e attore privato nell'elaborazione degli stessi, volti a coadiuvare gli operatori privati nell'adozione corretta del Regolamento[19].

Ebbene, proprio in questo ambito si nota una netta differenza rispetto alle fasi seguenti della co-regolazione della società digitale. I codici di condotta nella stagione del GDPR hanno una natura prettamente di *compliance* al Regolamento, ovvero svolgono un ruolo di guida, specie per quei titolari del trattamento di dimen-

[18] Così, G. Mobilio, *op. cit.*, p. 256.

[19] L'art. 40 GDPR, in particolare, prevede che spetta all'autorità nazionale competente – ovvero, al comitato europeo per la protezione dei dati (EDPB), qualora il codice di condotta riguardi più Stati membri – esprimere un parere sulla conformità del progetto di codice. Se il codice espleta le sue funzioni solo all'interno di un singolo Stato membro, spetta all'autorità nazionale competente approvare il codice. Qualora, invece, il codice ha una valenza transfrontaliera, e il parere dell'EDPB ritenga che il progetto di codice di condotta sia conforme al regolamento, il comitato trasmette il suo parere alla Commissione, la quale può decidere, mediante atti di esecuzione, di estendere la validità del codice a tutto il territorio dell'Unione.

sioni ridotte che potrebbero avere difficoltà nell'aderire alla tecnicità delle regole stabilite dal GDPR[20].

In linea con l'approccio flessibile delineato precedentemente, all'attore pubblico è riservato un ruolo marginale: egli non partecipa formalmente alla stesura del codice, ma si limita ad approvarne o respingerne il contenuto, una volta redatto dagli operatori del settore.

Alla luce dell'analisi fin qui esposta, emerge un quadro in cui l'attore pubblico opta per un approccio flessibile, laddove le misure tecniche e organizzative per il trattamento di dati personali vengono adottate, in primo luogo, dallo stesso titolare del trattamento. Tale approccio segue la logica di non rendere la regolazione troppo gravosa per il titolare del trattamento, lasciando spazi di manovra all'attore privato, in particolare affidando allo stesso il compito di decidere le modalità di intervento per garantire la tutela dei dati personali. L'azione dell'autorità pubblica si colloca, infatti, in una fase successiva, intervenendo solo qualora le modalità e le tecniche adottate dal titolare risultino non conformi al Regolamento, o comunque inadeguate a garantire pienamente i diritti e le libertà dell'interessato. In tale schema si coglie l'essenza del principio di *accountability* del titolare del trattamento, che rappresenta il cardine del modello co-regolatorio delineato dal GDPR.

Sulla base delle considerazioni sinora svolte, può osservarsi che, in questa prima fase, la co-regolazione può essere definita *a maglie larghe*: i nodi della rete della co-regolazione sono abbastanza distanziati da permettere all'attore privato di potersi muovere all'interno delle maglie. L'effetto prodotto è, da un lato, un ruolo più limitato esercitato dall'attore pubblico nell'orientare e dirigere i processi di innovazione digitale; dall'altro, il soggetto privato mantiene un significativo margine di autonomia nella regolazione e conduzione delle proprie attività.

---

[20] D'altronde, la scarsa percentuale di codici di condotta approvati a quasi dieci anni dall'entrata in vigore del GDPR evidenzia come tale strumento abbia una natura di mero strumento di ausilio all'operatore privato, restando dunque nel solco di uno strumento di *soft-regulation* di natura non vincolante. Si rinvia al GPDP, *Registro dei Codici di Condotta*, consultabile al link: *https://www.garanteprivacy.it/codici-di-condotta*.

## 3. *La co-regolazione a maglie strette nel Digital Package*

L'approccio regolativo muta nella seconda stagione della società digitale, caratterizzata dall'approvazione del *Digital Package*[21], all'interno della quale emerge un ruolo più incisivo dell'attore pubblico, in particolare della Commissione europea, nell'indirizzare e disciplinare le dinamiche del mercato digitale. Si inaugura, in tal modo, la fase di *co-regolazione a maglie strette*, caratterizzata da una maggiore densità degli obblighi normativi e da un più elevato grado di eterodirezione dei comportamenti privati.

Il *Digital Package* si compone di due regolamenti: il *Digital Services Act* (DSA)[22] e il *Digital Market Act* (DMA)[23].

Questi Regolamenti trovano la loro ragion d'essere nella consapevolezza del ruolo sistemico esercitato dalle grandi piattaforme digitali le quali, avendo consolidato posizioni dominanti nel mercato, pongono potenziali minacce sia al mercato, minando le fondamenta della libera concorrenza, sia ai diritti e alle libertà fondamentali degli individui.

Su queste premesse, l'attore pubblico europeo è intervenuto con i suddetti Regolamenti al fine di imbastire una regolazione che miri a regolare il mercato dei servizi digitali nel suo complesso (DSA), e un regolamento che miri a contrastare la concentrazione di potere economico in mano a pochi soggetti, denominati *gatekeeper* (DMA).

Per quanto concerne il DSA, questo Regolamento aggiorna la precedente Direttiva sul commercio elettronico[24] risalente agli anni

---

[21] Con la Comunicazione COM(2020) 825 final - *Digital Services Act package: Explanatory Memorandum*, la Commissione europea mira ad aggiornare le regole del mercato digitale, a 20 anni dalla Dir. 2000/31/CE (Direttiva e-Commerce), presentando il DSA e il DMA come strumenti per garantire trasparenza, equità e responsabilità delle piattaforme digitali, con il fine di tutelare i diritti fondamentali, promuovere un ambiente digitale sicuro e contenere il potere delle grandi piattaforme (*gatekeepers*).

[22] Reg. UE 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Dir. 2000/31/CE.

[23] Reg. UE 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 sui mercati contendibili e leali nel settore digitale e che modifica le Dir. 2019/1937/UE e 2020/1828/UE.

[24] Si fa riferimento alla Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società

2000, un lasso di tempo che nella società digitale è paragonabile, per così dire, ad ere geologiche, dato il forte dinamismo delle evoluzioni digitali. Dunque, era necessario intervenire per aggiornare concetti ormai desueti o comunque superati dall'innovazione tecnologica.

Tuttavia, il legislatore europeo non si è limitato a un semplice aggiornamento normativo, ma ha voluto affrontare anche le distorsioni esistenti nel mercato delle piattaforme digitali.

In linea di principio, il DSA ha l'obiettivo di garantire nell'ambiente online la stessa tutela prevista nell'ambiente offline[25]. Nel far questo, il DSA definisce nuove regole orizzontali, c.d. *due diligence*, necessarie per conseguire «*diversi obiettivi di interesse pubblico quali la sicurezza e la fiducia dei destinatari del servizio (digitale) e la tutela dei diritti fondamentali*»[26].

Inoltre, nel DSA si ritrova la stessa logica della regolazione *risk-based*, in quanto prevede obblighi di diversa natura e pregnanza a seconda del servizio offerto dalle piattaforme di intermediazione. In questo caso, però, la diversa natura degli obblighi deriva dalla diversa natura degli intermediari, in quanto la loro attività incide in maniera diversa sugli interessati[27].

Nello stabilire il regime di obblighi in capo agli intermediari, emerge il ruolo proattivo affidato all'attore pubblico, ovvero alla Commissione europea[28]. Essa svolge un ruolo di primo piano nella guida delle Autorità indipendenti degli Stati membri[29] e dispone di

---

dell'informazione, in particolare il commercio elettronico, nel mercato interno (Direttiva sul commercio elettronico), Gazzetta ufficiale n. L 178 del 17.7.2000.

[25] DSA, cons. 3.

[26] DSA, cons. 40.

[27] Il DSA prevede una differenziazione tra piattaforme di intermediazione *mere conduit, caching e hosting*, da cui ne discende una diversa categoria del rischio e quindi degli obblighi connessi.

[28] Traspare, inoltre, come obiettivo implicito del DSA, il contrasto allo strapotere dei grandi players della società digitale. Sul punto, M. OROFINO, *Il Digital Service Act tra continuità (solo apparente) ed innovazione*, in F. PIZZETTI *et al.*, *op. cit.*, p. 135. Questo obiettivo può essere raggiunto soltanto affidando la guida centrale all'organo politico (la Commissione) capace di poter trattare con questi grandi attori privati, in quanto se la guida fosse affidata ai singoli Stati membri si avrebbe una frammentazione delle scelte, con il rischio di dumping fiscale oltre che la tenuta stessa del mercato interno.

[29] È compito della Commissione valutare se sia opportuno esercitare o meno le competenze condivise, assumendo quindi una funzione di coordinamento e indirizzo nei confronti delle Autorità nazionali. Si veda DSA, cons. 124 e 125.

ampia discrezionalità per quanto concerne i poteri di indagine, esecuzione e monitoraggio[30].

Il ruolo della Commissione diventa ancora più marcato nel DMA, in quanto volto a contrastare la posizione dominante sul mercato delle grandi piattaforme digitali. Queste sono considerate come i baroni[31], ovvero i sovrani della rete[32], in quanto, grazie a costi marginali bassissimi e una forte economia di scala, riescono ad assumere una posizione dominante sul mercato. Tali piattaforme digitali, definiti dal DMA come *gatekeeper*, sono in grado di poter connettere migliaia di utenti commerciali con milioni di utenti finali, con una potenziale dipendenza sia degli uni che degli altri. In altre parole, queste piattaforme si sostituiscono al mercato, diventando esse stesse il mercato[33].

In virtù di ciò, l'obiettivo principale del DMA è quello di assicurare il corretto funzionamento del mercato interno, stabilendo norme armonizzate volte a tutelare le imprese che svolgono la propria attività nel settore digitale in cui è presente uno o più *gatekeeper*[34].

A tal proposito, all'interno del DMA è previsto un articolato elenco di divieti (*don'ts*) volti a vietare comportamenti lesivi dell'equità del mercato e l'imposizione di obblighi (*dos*) in capo ai *gatekeeper*, al fine di garantire la concorrenza nel mercato di riferimento[35].

---

[30] DSA, cons. 138, 139 e 140.

[31] Il riferimento è al volume di M. Betzu, *I baroni del digitale*, Editoriale scientifica, Napoli, 2022.

[32] Cfr. F. Paruzzo, *I sovrani della rete. Piattaforme digitali e limiti costituzionali al potere privato*, Edizioni Scientifiche Italiane, Torino, 2022.

[33] Come è stato giustamente osservato, «*le piattaforme di maggior successo non sono semplici attori di mercato né banalmente estendono i mercati esistenti, ma più radicalmente li sostituiscono, dettando esse stesse le condizioni tecnologiche e giuridiche che presiedono allo svolgimento degli scambi*». Così, G. Resta, *op. cit.*, p. 1023.

[34] Del resto, il DMA sancisce (in maniera esplicita) l'intento di contrastare lo strapotere delle grandi piattaforme digitali (gatekeeper) al fine di garantire che i mercati del settore digitale siano effettivamente contendibili ed equi a favore degli utenti commerciali e degli utenti finali. DMA, art. 1.1.

[35] Gli obblighi si trovano nel testo del DMA, art. 5, pp. 4, 5, 9, 10. I termini tra parentesi sono tratti da M. Orofino, *Il Digital Market Act: una regolazione asimmetrica*

A vigilare sul rispetto di tali «*don'ts e dos*» è, ancora una volta, la Commissione. Sul punto, il DMA afferma che la Commissione europea viene designata come «*l'unica autorità incaricata di applicare il presente regolamento*»[36].

Per assolvere a tale funzione, il Capo V del DMA è dedicato interamente ai numerosi compiti della Commissione, in merito ai poteri di indagine, di esecuzione, di monitoraggio e sanzionatori[37].

Alla luce di quanto riportato finora, all'interno del *Digital Package*, la Commissione assume una posizione centrale e di rilievo nel governo della regolazione dei mercati digitali, con la facoltà di intervenire direttamente sugli operatori per garantire il rispetto delle norme e orientare l'evoluzione del settore.

Tale accentramento di funzioni in capo alla Commissione si riscontra, finanche, nell'adozione dei codici di condotta previsti dal DSA. A tal proposito, si rileva una natura trasformativa più profonda dei codici di condotta: essi devono prevedere, *ab origine*, meccanismi per il conseguimento degli «*obiettivi di interesse pubblico*»[38] del Regolamento e la loro adozione è soggetta al controllo

---

*a cavallo tra diritto della protezione dati e diritto antitrust*, in F. Pizzetti *et al.*, *op. cit.*, pp. 175-198.

[36] DMA, cons. 91. Questo approccio supera il modello precedente basato sul controllo esercitato dalle singole autorità indipendenti degli Stati membri. In effetti, l'assetto precedente previsto nel GDPR, fondato su meccanismi di concerto e coordinamento tra le diverse autorità (con l'individuazione di autorità capofila in riferimento allo stabilimento principale ove la piattaforma esercita la sua attività), appare inadeguato di fronte alla natura transnazionale delle grandi piattaforme digitali.

[37] Anzitutto, spetta alla Commissione adottare l'avvio di un procedimento, richiedere informazioni utili per l'assolvimento dei compiti previsti dal regolamento, procedere alle audizioni. A seguito della raccolta delle informazioni sulla natura concorrenziale del mercato, la Commissione può effettuare le ispezioni necessarie, e quindi accedere ai locali, esaminare i libri contabili dell'impresa, richiedere l'accesso al funzionamento del sistema informatico, alla gestione dei dati, alle pratiche commerciali dell'impresa. Inoltre, nei casi di urgenza dovuti ad un rischio elevato per gli utenti commerciali e finali, la Commissione può adottare misure provvisorie (solo per un determinato periodo di tempo). Ancora, spetta alla Commissione il monitoraggio degli obblighi previsti dal regolamento, con l'obbligo per il gatekeeper di conservare tutti i documenti ritenuti pertinenti per valutare l'aderenza dello stesso ai divieti e agli obblighi del DMA. Infine, spetta alla Commissione irrogare sanzioni, il cui importo non supera il 10% del fatturato totale, oppure del 20% del fatturato totale qualora il gatekeeper sia recidivo nel commettere una infrazione già constatata.

[38] DSA, cons. 103.

pubblico (della Commissione). In altri termini, si sancisce un sostanziale invito alle parti interessate (le piattaforme) ad elaborare codici e linee guida, qualora vi sia un *rischio sistemico* significativo in cui emerge chiaramente una rilevanza pubblicistica[39]. Infatti, qualora si riscontrasse un *rischio sistemico*, ai sensi dell'art. 34 DSA, – ovvero, inerente la diffusione di contenuti illegali online, il prodursi di effetti negativi, attuali o prevedibili, sui diritti fondamentali, sul dibattito civico, i processi elettorali, la sicurezza pubblica, la violenza di genere, la protezione della salute pubblica e dei minori, il benessere fisico e mentale della persona – la Commissione può invitare le piattaforme digitali all'elaborazione di codici di condotta «*stabilendo impegni ad adottare misure specifiche di attenuazione dei rischi nonché un grado di comunicazione periodica sulle misure adottate e sui relativi risultati*»[40].

Si evince, così, una *funzione pubblicistica* affidata ai codici di condotta, in modo che gli attori privati nella redazione delle proprie regole tengano conto dei potenziali rischi per la collettività[41].

Ebbene, sulla base delle considerazioni fin qui svolte, nella stagione del *Digital Package* sembra delinearsi un restringimento delle maglie della rete regolatoria: i nodi della regolazione appaiono più ravvicinati, in quanto si accentua il ruolo dell'attore pubblico, il quale non si affida esclusivamente alla responsabilizzazione dell'attore privato, piuttosto lo indirizza finanche alla redazione di regole volte alla tutela della collettività.

Si assiste, così, al passaggio da una *co-regolazione a maglie larghe*, come descritta nel GDPR, ad una *co-regolazione a maglie strette* nel *Digital Package*, in quanto si riscontra, in primo luogo, un ruolo più influente dell'attore pubblico e, in secondo luogo, sono più specifici e marcati gli obblighi in capo alle piattaforme digitali.

---

[39] Sul punto si rinvia a M. Bassini, *L'unione europea al grande passo: verso una regolamentazione di mercati e servizi digitali*, in *Quaderni Costituzionali*, 1, 2021.

[40] DSA, art. 45.

[41] Tale aspetto non è esente da critiche, dato che, in materia di diritti fondamentali della persona in relazione all'ecosistema digitale, ampi spazi di manovra sono lasciati all'attore privato. Si rinvia a N. Maccabiani, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e di sostanza*, in *Osservatorio sulle fonti*, 3, 2022, in particolare, pp. 77-79.

## 4. *La co-regolazione nell'AI Act*

Ad oggi, la regolazione della società digitale è di fronte ad un'altra sfida decisiva: non riguarda esclusivamente la protezione e la circolazione dei dati personali, come nel GDPR, né la piattaforma digitale che utilizza tali dati, come nel *Digital Package*. Piuttosto è rivolta alla potenza di calcolo, ovvero alla capacità computazionale del flusso di dati, quella che comunemente è chiamata Intelligenza artificiale[42].

Questo nuovo scenario pone sfide inedite alla regolazione. Da un lato, affidare agli attori privati, tramite una *co-regolazione a maglie larghe*, l'adozione delle misure idonee a gestire le tecnologie di AI può produrre effetti pregiudizievoli non solo per gli individui, ma finanche per i valori e i principi alla base delle istituzioni democratiche[43]. Dall'altro lato, se si opta per una *co-regolazione a maglie strette*, in cui l'attore pubblico assume un ruolo preponderante, in assenza però delle adeguate competenze tecniche, si rischia di frenare l'innovazione dell'AI, con una potenziale ricaduta sui diritti degli individui, come già affermato precedentemente[44].

Pertanto, la scelta del modello di co-regolazione da adottare nell'ambito dell'AI dovrebbe muovere dalle potenzialità di entrambe le strategie, combinandone in modo equilibrato gli elementi caratterizzanti. In particolare, è opportuno prevedere una regolazione a maglie larghe, fondata sulla responsabilizzazione degli operatori dell'intelligenza artificiale, così da favorire l'innovazione e la sperimentazione tecnologica; ma, al contempo, mantenere la possibilità di ricorrere, qualora le circostanze lo richiedano, a una co-regolazione a maglie strette, capace di indirizzare il progresso tecnologico e di tutelare gli interessi fondamentali delle comunità umane.

---

[42] Naturalmente, è bene precisare che al centro dell'intervento regolatorio non vi è la tecnologia in quanto tale, bensì gli effetti che essa genera, o può generare, sui diritti fondamentali, sulla democrazia, sull'equilibrio tra i poteri e, più in generale, sull'idea stessa di spazio pubblico.

[43] Sul punto si veda A. Pajano *et al.*, *op. cit.*, pp. 205-235; Ancora, si rinvia a G. Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giurisprudenza italiana*, luglio 2019, pp. 1670-1677; F. Pizzetti, *Intelligenza Artificiale, Protezione Dei Dati Personali e Regolazione*, Giappichelli, Torino, 2018.

[44] *Supra*, par. 1.

Ebbene, proprio su questa dicotomia sembra muoversi il regime co-regolatorio dell'AI Act, ossia combinare la flessibilità della *co-regolazione a maglie larghe* con la rigidità della *co-regolazione a maglie strette*.

Come è stato opportunamente osservato, la regolazione delle tecnologie di AI si realizza attraverso un approccio normativo stratificato di livello superiore di requisiti e di obblighi che necessita di essere integrato da standard armonizzati e codici di condotta, consentendo così la flessibilità necessaria per adattare le regole allo sviluppo tecnologico[45].

Con riferimento al regime solido della regolazione, esso si concretizza nel ruolo proattivo dell'attore pubblico, il quale delinea una trama fitta e coerente di obblighi a carico degli operatori dell'intelligenza artificiale, orientando in modo diretto lo sviluppo e l'impiego di tali tecnologie.

L'AI Act, nella definizione degli obblighi, segue il classico approccio *risk-based*, individuando le pratiche sempre vietate; il rischio elevato, il rischio basso o minimo a cui segue un generale obbligo di trasparenza. Parimenti, con riferimento ai modelli di AI per finalità generali (GPAI), si individuano obblighi specifici in merito il rischio correlato al suo utilizzo, il quale non viene definito alto, bensì sistemico[46]. Il rischio sistemico non costituisce una categoria autonoma di classificazione del rischio, bensì si innesta come elemento integrativo sulla qualificazione già attribuita al sistema di AI[47].

---

[45] Si rinvia a R.W. DE BRUIN, *Co-regulation and AI-Innovation: Principles for a Sustainable Framework Fostering Innovation and Acceptance of AI*, in M.I. ALDINHAS FERREIRA, *Producing Artificial Intelligent System* (edited by), vol. 1150, Springer, Switzerland, 2024, pp. 119-140.

[46] Data la complessità della nozione di rischio sistemico, la prima sezione del Capo V è dedicata all'individuazione e classificazione dei modelli di AI per finalità generali a rischio sistemico, indicando all'art. 52 la procedura secondo cui la Commissione può designare tale modello come potenzialmente a rischio sistemico.

[47] Il cons. 97 AIA indica, infatti, che i sistemi di AI che incorporano modelli di AI a finalità generali sono soggetti sia agli obblighi previsti in relazione alla categoria di rischio del sistema (alto o basso), sia a quelli specifici per i modelli a finalità generali. Ancora, il cons. 110 AIA riporta che «*i modelli di AI per finalità generali potrebbero comportare rischi sistemici che includono, tra l'altro, qualsiasi effetto negativo effettivo o ragionevolmente prevedibile in relazione ad incidenti gravi, perturbazioni di settori critici e serie conseguenze per la salute e la sicurezza pubbliche,* [oltreché] *per i processi*

Per quanto concerne il rischio elevato, l'AI Act prevede una dettagliata lista di requisiti per l'individuazione dei sistemi di AI a rischio elevato[48], da cui ne discendono specifici e dettagliati obblighi. A tal riguardo, l'art. 16 AI Act schematizza e riassume tali obblighi in capo ai fornitori di sistemi di AI ad alto rischio.

Il complesso dei requisiti e degli obblighi previsti dall'AI Act comprende: la gestione del rischio, la garanzia della qualità e della tracciabilità dei dati, la predisposizione della documentazione tecnica, la trasparenza nei confronti degli utenti, la supervisione umana, nonché la robustezza e la sicurezza dei sistemi. A tali adempimenti si aggiungono, inoltre, la registrazione e la valutazione di conformità, mentre, per i modelli di base più influenti, sono previsti ulteriori obblighi[49], quali l'analisi continua dei rischi, gli audit in-

---

*democratici e la sicurezza pubblica ed economica*». Pertanto, il rischio che tali modelli possono generare non riguarda (solo) un rischio per il singolo individuo, piuttosto ha una ricaduta potenziale sull'intera collettività, tanto da comparare il rischio derivante dall'utilizzo distorto di tali modelli di AI con i rischi chimici, biologici, radiologici e nucleari.

[48] Tali requisiti riguardano: *a*) un sistema di gestione dei rischi (art. 9); *b*) misure di governance e gestione dei dati (art. 10); *c*) predisposizione di documentazione tecniche (art. 11); *d*) la registrazione automatica di tutte le attività svolte dalla macchina in modo da monitorarne il funzionamento (art. 12); *e*) la trasparenza (art. 13); *d*) la sorveglianza umana (art. 14); infine, riguardano i parametri della progettazione di sistemi di AI, i quali devono rispondere ai requisiti di accuratezza, robustezza e cybersicurezza (art. 15). Per un'analisi dettagliata dei requisiti suesposti, si rinvia a E. LONGO, *Le pratiche di AI vietate e i sistemi di Ai ad alto rischio*, in F. PIZZETTI *et al.*, *op. cit.*, pp. 76-79.

[49] In primo luogo, è previsto l'obbligo di conformarsi ai requisiti sopra menzionati, stabiliti nella Sez. 2. In secondo luogo, i soggetti devono indicare la propria denominazione commerciale registrata o il marchio, nonché l'indirizzo al quale possono essere contattati.

Il terzo obbligo riguarda l'adozione di un sistema di gestione della qualità, disciplinato in modo puntuale dall'art. 17 AIA. Il quarto concerne la conservazione della documentazione, oggetto di specifica regolamentazione nell'art. 18. A ciò si aggiunge l'obbligo di conservare i log, qualora siano generati automaticamente, secondo quanto previsto dall'art. 19.

È inoltre previsto l'obbligo di garantire che i sistemi ad alto rischio siano sottoposti a valutazione di conformità, ai sensi dell'art. 43, prima della loro immissione sul mercato. A ciò si accompagnano l'obbligo di redigere una dichiarazione di conformità UE (art. 47) e quello di apporre la marcatura CE.

Ulteriori obblighi comprendono: il rispetto delle prescrizioni di cui all'art. 49, par. 1 (in merito alla registrazione); la fornitura delle informazioni necessarie confor-

dipendenti, la presentazione di report periodici alla Commissione europea e la cooperazione con l'AI Office. Il rispetto di tali obblighi è dirimente per l'ingresso di queste tecnologie nel mercato europeo[50].

Tuttavia, il regime solido della regolazione, fin qui delineato, assume un carattere flessibile grazie alla previsione di sistemi di standardizzazione e di norme armonizzate oltre che alla possibilità, riconosciuta agli operatori del settore, di elaborare procedure autonome di valutazione delle stesse, purché conformi ai criteri stabiliti dal regolatore europeo.

Come detto, l'AI Act definisce i requisiti dei sistemi di AI ad alto rischio; tuttavia, la loro specificazione tecnica è affidata ad organismi tecnici di settore, quali gli *European Standardization Organizations* (ESOs). In tal modo, questi enti privati a funzione pubblica svolgono un ruolo cruciale nell'applicazione coerente dell'AI Act, in quanto hanno il compito di definire, attraverso l'elaborazione di standard armonizzati, i criteri per l'individuazione e la classificazione dei sistemi ad alto rischio.

In altri termini, la Commissione europea si fa carico di predisporre le richieste di normazione relative ai requisiti previsti dal Capo III, sezione 2 e agli obblighi contemplati nel Capo V, sezioni 2 e 3. A tale processo di normazione, tuttavia, è prevista la parteci-

---

memente all'art. 20 (relative a misure correttive e al dovere di informazione); infine, l'onere di dimostrare la conformità ai requisiti della Sezione 2, qualora ciò sia richiesto in modo motivato da un'autorità nazionale, come disciplinato, in maniera più puntuale all'art. 21.

Oltre agli obblighi per i fornitori, sono previsti specifici obblighi anche per gli importatori (art. 23), per i distributori (art. 24) e per i deployer (art. 26), oltreché la specifica responsabilità di ognuno entro la catena del valore (art. 25).

[50] Tale disciplina richiama in maniera significativa il modello normativo previsto per la sicurezza dei prodotti. Cfr., E. LONGO, *op. ult. cit.*, p. 71. A tal proposito, il regime solido di regolazione, si arricchisce della proposta della Commissione di aggiornare la precedente Direttiva 85/374/CEE sulla sicurezza dei prodotti alla luce degli sviluppi dell'AI. Da questa proposta è scaturita la Direttiva UE 2024/2853 sulla responsabilità per danni da prodotti difettosi, del 23 ottobre 2024. Tale Direttiva riconosce, infatti, che è necessario intervenire per aggiornare la normativa precedente alla luce degli sviluppi legati all'AI, evidenziando che «*l'esperienza maturata ha dimostrato che per il danneggiato è difficile ottenere il risarcimento del danno subito, soprattutto a causa della crescente complessità tecnica e scientifica*».

pazione degli operatori del settore[51], i quali – in virtù delle loro competenze tecniche e della conoscenza diretta delle dinamiche di sviluppo delle tecnologie di intelligenza artificiale – contribuiscono attivamente alla definizione degli standard tecnici concernenti i medesimi requisiti e obblighi cui essi stessi saranno soggetti.

A tal riguardo, l'art. 40 AI Act disciplina la predisposizione di norme armonizzate. La norma armonizzata è una norma europea adottata sulla base di una richiesta della Commissione, elaborata da enti privati a funzione pubblica, le già citate ESOs (quali CEN, CENELEC, ETSI)[52]. In altre parole, una norma armonizzata è una norma tecnica adottata da un organismo (privato) europeo di normazione, su mandato della Commissione europea, in applicazione della legislazione di armonizzazione dell'Unione.

Tale aspetto non è privo di critiche[53]. D'altronde, questi organismi di standardizzazione sono organizzazioni private e burocratiche in cui vi rientrano anche numerose multinazionali, i cui interessi non coincidono pienamente con i valori dell'UE. Come è stato osservato, «*le ESOs mancano di rappresentanza e di un coinvolgimento significativo della società civile (specialmente a livello nazionale), delle autorità per la protezione dei dati, degli esperti in accessibilità, dei gruppi per i diritti dei consumatori e di altri stakeholder rilevanti o impattati*»[54].

Da quanto precede, si può rilevare come le norme armonizzate, in tale contesto, assumono un ruolo cruciale: data la comples-

---

[51] AIA, art. 40, p. 3.

[52] AIA, art. 3, p. 27.

[53] A tal riguardo, si ritiene che, «*se da un lato gli standard armonizzati sono importanti per facilitare la conformità tecnica uniforme dei fornitori a determinati requisiti dell'UE, dall'altro il progetto di AI Act non dovrebbe delegare alcuna decisione agli organismi di standardizzazione che possa incidere su punti chiave politici e giuridici*». Sul punto, ESRI, *The Role of Standards and Standardization process in the EU's Artificial Intelligence*, consultabile al link: *https://edri.org/wp-content/uploads/2022/05/The-role-of-standards-and-standardisation-processes-in-the-EUs-Artificial-Intelligence-AI-Act.pdf*.

[54] *Ibidem*. Del resto, il processo di standardizzazione comporta due problemi fondamentali: da un lato vi la mancanza di legittimazione politica degli organismi tecnici di standardizzazione, a cui si lega anche una mancanza di controllo politico; dall'altro, tali organi non considerano le implicazioni di natura non tecnica. Sul punto, si rinvia a G. Mobilio, *L'intelligenza artificiale e i rischi di una "disruption" della regolazione giuridica*, in *BioLaw Journal - Rivista di BioDiritto*, 2, 2020, pp. 401-424.

sità tecnica della materia, esse, pur essendo «*uno strumento politico per governare il mercato dell'AI*»[55], derivano marcatamente dal contributo degli esperti del settore.

A rafforzare tale impostazione si aggiunge il fatto che l'art. 43 AI Act detta disposizioni in merito alla valutazione di conformità rispetto alle norme armonizzate. A tal proposito, eccetto i prodotti dell'Allegato I, sez. A, in cui si prevede l'armonizzazione secondo gli atti giuridici indicati, sono previsti altri meccanismi di valutazione: il primo di autovalutazione del fornitore, contenuta nell'Allegato VI (controllo interno); il secondo tramite la valutazione di soggetti terzi, contenuta nell'Allegato VII (valutazione da parte di organismi notificati)[56]. A seguito della valutazione (o autovalutazione) di conformità, viene rilasciato un certificato (art. 44 AI Act) e viene applicato il marchio CE (art. 48 AI Act). Pertanto, si affida ad organismi privati l'analisi e la valutazione degli effetti delle tecnologie di AI, finanche, sui diritti fondamentali[57].

Sulla base di quanto finora analizzato, si può osservare che l'AI Act assegna un compito dirimente agli esperti del settore, chiamati a definire in concreto i requisiti tecnici e gli standard applicabili ai sistemi e ai modelli di intelligenza artificiale. In tale prospettiva, mentre all'attore pubblico spetta la competenza di stabilire gli obblighi generali, la determinazione operativa di tali obblighi è ri-

---

[55] […] *che si applicano anche quando i produttori hanno deciso di non affidarsi ad esse*». Infatti, qualora le norme armonizzate non trovino seguito, l'art. 41 AIA prevede che, laddove insufficienti o laddove vi sia la necessità di intervenire per questioni di sicurezza o di diritti fondamentali, la Commissione può adottare atti di esecuzione che stabiliscano specifiche comuni. Permane, dunque, la netta volontà politica delle istituzioni europee di orientare il processo volto a immettere sul mercato prodotti di AI affidabili. Sembra, pertanto, che la Commissione continui il suo percorso nel rafforzamento del suo ruolo nella regolazione della società digitale, laddove vi è un intervento maggiore «*di ordine pubblicistico volto a tradursi in un restringimento dell'ambito di manovra dell'autonomia privata*». Così, E. Longo, *op. ult. cit*., p. 88.

[56] AIA, art. 43, pp. 1 e 2.

[57] Da cui ne discendono dubbi circa la reale aderenza ai parametri di conformità richiesti. Sul punto si rinvia a M. Veale *et al.*, *Demystifyng the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach*, in *Computer Law Review International*, 4, 2021. Ancora, si veda M. Ebers *et al.*, *The European Commission's Proposal for an Artificial Intelligence Act. A Critical Assessment by Members of the Robotics and AI Law Society*, in *Multidisciplinary Scientific Journal*, 4, 2021.

messa agli stessi soggetti privati cui essi sono destinati, i quali concorrono così alla strutturazione effettiva del quadro regolatorio.

Si delinea così un modello di co-regolazione dinamico, in cui i ruoli dell'attore pubblico e di quello privato risultano interconnessi e reciprocamente condizionati. Tale aspetto sembra emergere, finanche, nella predisposizione dei codici di buone pratiche, di cui il Capo IV, sez. 4, dedica ampio spazio.

A tal riguardo, l'art. 56 AI Act afferma che l'AI Office incoraggia e agevola l'elaborazione di codici di buone pratiche, favorendo la partecipazione, oltre che dei fornitori di modelli di AI per finalità generali, anche le pertinenti autorità nazionali, le organizzazioni della società civile, l'industria, il mondo accademico e altri pertinenti portatori di interesse. Una volta elaborato il codice, spetta alla Commissione approvarlo, mediante atto di esecuzione, in modo da conferire ad esso una validità generale all'interno dell'Unione[58].

A tal proposito, il 10 luglio 2025 è stata pubblicata la versione finale del primo codice di condotta per le aziende che sviluppano e utilizzano intelligenza artificiale per finalità generali, GPIA[59].

Tale codice è progettato per orientare gli operatori nel processo di conformazione alle disposizioni previste dall'AI Act per i modelli di intelligenza artificiale a finalità generali[60]. A tal fine, il codice for-

---

[58] Come è stato opportunamente osservato, «tale approvazione successiva sfuma la natura co-regolatoria dell'atto, finendo con limitare il ruolo dei fornitori solo alla prima fase di drafting del Codice». Sul punto, M. Orofino, *La regolazione dei modelli di AI per finalità generali*, in F. Pizzetti *et al.*, *op. cit.*, p. 106.

[59] Si tratta di uno strumento volontario elaborato da un *Working Group* composto da 13 esperti indipendenti, con il contributo di oltre 1.000 stakeholder, tra cui fornitori di modelli, piccole e medie imprese, accademici, specialisti di sicurezza dell'IA, titolari di diritti e organizzazioni della società civile. Si veda, Commissione europea, *Comunicato stampa: Il codice di buone pratiche dell'IA per finalità generali è ora disponibile*, Bruxelles, 10 luglio 2025. Si rinvia al link: *https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1787*.

[60] Come noto, il Regolamento sull'Intelligenza Artificiale, in vigore dal maggio 2024, prevede un'applicazione graduale nel tempo, così da consentire alle imprese di adottare le misure necessarie per conformarsi alle sue disposizioni. L'art. 113 del Reg. UE 2024/1689 (AI Act), che ne costituisce la disposizione finale, prevede, alla lettera *b*), che a partire dal 2 agosto 2025 diventino applicabili: il capo III, sezione 4 (Autorità di notifica e organismi notificati), il capo V (modelli di AI per finalità generali), il capo VII (governance), il capo XII (sanzioni) e l'art. 78 (riservatezza), con la sola

nisce un quadro di riferimento che consente a produttori, distributori, importatori e deployers di modelli GPIA di garantire la conformità alle prescrizioni del Regolamento[61]. In particolare, si sofferma su tre elementi specifici: trasparenza, copyright e sicurezza[62].

Seppur il codice di condotta mantiene una natura prettamente volontaristica, nell'ambito della regolazione dell'AI esso assume una valenza più profonda, divenendo uno strumento *necessario* per gli operatori in modo che essi possano dimostrare di essere conformi agli obblighi del Regolamento[63].

---

eccezione dell'art. 101, relativo alle sanzioni pecuniarie per i fornitori di modelli di AI per finalità generali.

[61] La natura di questo codice, secondo l'impostazione data dalla Commissione, è di essere un documento guida per la conformità agli obblighi previsti dagli artt. 53 e 55 AIA, garantire che i fornitori di modelli di AI per finalità generali si adeguino alle prescrizioni dell'AIA e facilitare l'AI Office nella valutazione di conformità. Così, G. BORGOGNONE, A. CATALETA, *AI Act, ecco il codice di condotta per GPAI: come usarlo per adeguarsi*, in *Agenda Digitale*, 10 luglio 2025, disponibile su: *https://www.agendadigitale.eu/industry-4-0/ai-act-ecco-il-codice-di-buone-pratiche-come-usarlo-per-adeguarsi/#_ftn2*.

[62] Il capitolo dedicato alla Trasparenza fornisce un modello di documentazione standard, di facile utilizzo, che consente ai fornitori di raccogliere in un unico documento tutte le informazioni necessarie. Il capitolo sul Copyright offre, invece, soluzioni pratiche per adottare politiche pienamente conformi alla normativa europea in materia. Poiché alcuni modelli di IA a finalità generali possono generare rischi sistemici, tra cui minacce ai diritti fondamentali e alla sicurezza, fino alla possibilità di agevolare lo sviluppo di armi chimiche o biologiche, o la perdita di controllo sul modello, l'AI Act impone ai fornitori l'obbligo di valutarli e mitigarli. A tal fine, il capitolo Sicurezza e protezione raccoglie le migliori pratiche disponibili per la gestione di tali rischi. Sul punto, Commissione europea, *Comunicato stampa: Il codice di buone pratiche dell'IA per finalità generali è ora disponibile*, Bruxelles, 10 luglio 2025, link: *https://ec.europa.eu/commission/presscorner/detail/it/ip_25_1787*.

[63] L'adozione del Codice di condotta per modelli GPIA costituisce uno step decisivo nella messa in opera dell'AI Act. La richiesta di conformità agli obblighi previsti dal Regolamento risponde all'esigenza di rendere l'AI il più possibile sicura e affidabile per gli utilizzatori finali, in linea con l'obiettivo principale del Regolamento, ovverosia promuovere la diffusione di un'AI antropocentrica e affidabile, rispettosa dei diritti fondamentali riconosciuti dalla Carta dei Diritti fondamentali dell'Unione Europea. Al tempo stesso, data la duttilità dei modelli GPAI, è indispensabile richiedere la partecipazione attiva degli stakeholder e degli esperti del settore, in modo da impostare una regolazione capace di cogliere le innovazioni future e di adattarsi dinamicamente alla loro evoluzione.

Proprio la costante innovazione e trasformazione delle tecnologie di intelligenza artificiale porta l'attore pubblico europeo ad intervenire secondo un approccio regola-

La natura necessaria dei codici di condotta all'interno del quadro regolatorio fornito dall'AI Act si ravvisa, in particolare, dalla previsione dell'art. 55 AI Act, la quale, in merito agli obblighi dei fornitori di modelli di AI per finalità generali con rischio sistemico, chiarisce che questi, per dimostrare la conformità a tali obblighi, possono basarsi su codici di buone pratiche, fino alla pubblicazione di una norma armonizzata. Si precisa, inoltre, che coloro che non aderiscono a un codice di buone pratiche devono, comunque, dimostrare con mezzi alternativi adeguati, la conformità ai fini della valutazione da parte della Commissione.

Pertanto, il codice di condotta sembra fungere da parametro di riferimento entro cui valutare la conformità o meno agli obblighi imposti dall'attore pubblico all'attore privato. Ai sensi dell'art. 56 dell'AI Act, è infatti previsto che, qualora entro il 2 agosto 2025 tale codice non fosse stato adottato, o qualora l'AI Office non lo avesse ritenuto idoneo, sarebbe spettato alla Commissione intervenire, mediante atti di esecuzione, predisponendo norme comuni per l'attuazione degli obblighi di cui agli artt. 53 e 55 AI Act. Ne consegue che gli operatori privati sono stati fortemente incentivati a partecipare attivamente alla redazione del codice di condotta, così da assicurare la propria conformità agli obblighi previsti e, al contempo, contribuire alla definizione concreta del quadro regolatorio dell'intelligenza artificiale.

Come è stato opportunamente osservato, il codice di condotta nella stagione dell'AI Act, «*si configura come uno snodo strategico nel tentativo di tradurre l'ambizione regolativa in prassi operative. Il suo carattere volontario, infatti, è solo apparente: in un contesto giuridico fortemente asimmetrico, l'adesione al Codice diventa il passaggio quasi obbligato per chi voglia dimostrare in via anticipata la conformità dei propri processi agli standard europei*»[64].

---

tivo che tende a combinare l'aspetto flessibile, dato dai codici di condotta, con quello solido, dato dall'imposizione di specifici obblighi. Tale approccio si rende necessario per non arrestare l'innovazione tecnologica e, al tempo stesso, garantire il rispetto dei diritti fondamentali degli individui, messi a rischio da un potenziale uso indiscriminato delle nuove tecnologie digitali.

[64] Così, O. Pollicino, *AI Act, Pollicino: "Codice di Condotta embrione di una nuova grammatica costituzionale"*, in *AgendaDigitale.eu*, 5 agosto 2025, consultabile al

Alla luce di ciò, è reso manifesto il significato del considerando 117 dell'AI Act, il quale definisce il codice di condotta come «*uno strumento essenziale*»[65] per i fornitori di modelli di AI per finalità generali[66].

Così, il codice di condotta, in questa nuova stagione, si configura come uno strumento dotato di una nuova valenza normativa: esso rappresenta un requisito *necessario ed essenziale* per l'applicazione del Regolamento sull'AI, in quanto, combinando le conoscenze tecniche degli operatori di settore con la direzione e il controllo dell'attore pubblico, rappresenta un elemento imprescindibile per garantire la corretta implementazione delle disposizioni normative.

In definitiva, i codici di condotta, hanno il compito di «*tradurre la prassi regolatoria in regole applicative*»[67].

Alla luce delle considerazioni svolte, è possibile individuare un modello di *co-regolazione ibrida*, in cui i nodi della rete della regolazione si allargano e si restringono, con riguardo sia al rischio per gli individui, sia al livello di tecnicità richiesta.

In particolare, emerge come il ruolo proattivo dell'attore pubblico si traduca nella definizione di un articolato sistema di obblighi a carico dei sistemi e modelli di AI, volto a garantire la tutela sia dell'individuo sia della collettività, nonché a incentivare gli operatori privati all'adesione agli obblighi stessi tramite i codici di condotta. Al tempo stesso, si rileva un ruolo cruciale dell'attore privato nella redazione tecnica delle norme a cui egli stesso deve conformarsi, contribuendo non solo alla loro applicazione pratica, ma anche alla loro adattabilità e aggiornamento continuo, in modo da rendere la regolazione dinamica e coerente con l'evoluzione tecnologica e del mercato.

---

link: *https://www.agendadigitale.eu/cultura-digitale/ai-act-pollicino-codice-di-condotta-embrione-di-una-nuova-grammatica-costituzionale/*.

[65] AIA, cons. 117.

[66] L'art. 53.4 AIA afferma che i modelli di AI per finalità generali possono basarsi su codici di buone pratiche per dimostrare la conformità agli obblighi finché non è pubblicata una norma armonizzata. Allo stesso modo, l'art. 55.2 AIA riporta la stessa affermazione in relazione ai modelli di AI con rischio sistemico.

[67] Così, O. POLLICINO, *op. ult. cit.*

## 5. *La co-regolazione nell'AI Act, assimilabile a una sfera di Hoberman*

Dall'analisi svolta nei paragrafi precedenti si è cercato di dimostrare come le maglie della co-regolazione hanno cominciato a restringersi per adeguarsi al rischio delle nuove tecnologie digitale.

Si è passati da una fase di *co-regolazione a maglie larghe* nella stagione del GDPR, basata sul principio di *accountability* del titolare del trattamento, ad una *co-regolazione a maglie strette*, giustificata dall'imposizione nel mercato di determinate piattaforme digitali.

Il GDPR, come noto, accanto all'obiettivo della protezione dei dati personali, garantisce la massima circolazione degli stessi, in quanto, il dato rappresenta l'elemento alla base per far evolvere la società digitale. In questo contesto era necessario mantenere al minimo gli oneri in capo alle aziende in modo da non frenare l'innovazione digitale. Inoltre, la co-regolazione flessibile prevista nel GDPR si giustifica per il fatto che, seppur riferita ai titolari (e responsabili) del trattamento, questi restano indefiniti, in quanto vi rientrano tutti coloro che trattano i dati personali degli individui.

Di converso, l'approccio co-regolatorio rigido che emerge nel *Digital Package*, è stato possibile soprattutto perché l'ambito normativo – incentrato sulla tutela della concorrenza di mercato – è storicamente familiare alla matrice eurounitaria, essendo questo uno degli obiettivi primari e fondanti del processo di integrazione europea. Inoltre, tale regolazione si rivolge a soggetti ben definiti, ovvero le piatteforme digitali[68]. Di conseguenza, la regolazione in questo settore è risultata più agevole, poiché rivolta non tanto, e non solo, alla protezione dei dati e alla loro circolazione, bensì a soggetti ben definiti che agiscono sul mercato, fattore, questo, che ha facilitato la loro identificazione e la conseguente applicazione delle norme[69].

---

[68] Ad esempio, il DMA, *ex* art. 3, elenca dei precisi requisiti per la designazione dei gatekeeper. Parimenti, il DSA, agli artt. 4, 5 e 6, individua le diverse categorie di intermediari, alle quali vengono attribuiti obblighi specifici e differenziati.

[69] L'enforcement dei Regolamenti in oggetto mostra un certo grado di reattività. Infatti, sono state comminate alcune multe significative, come quella da 500 milioni di euro inflitta ad Apple per la violazione del DMA e una multa da 345 milioni di euro a TikTok per violazioni correlate al DSA. A proposito si rinvia a U. GAMBINI, A. MASSOLO, F. RICCHI, *DMA, Ue all'attacco: cosa cambia dopo le maxi sanzioni a Apple e Meta*,

Ebbene, nella nuova fase della società digitale, caratterizzata dalla diffusione dirompente delle tecnologie di intelligenza artificiale, emergono tutti gli elementi che hanno contraddistinto la regolazione nelle fasi precedenti.

In primo luogo, risulta fondamentale favorire l'innovazione delle tecnologie di AI, poiché, seguendo l'impostazione della libera circolazione dei dati delineata nella stagione del GDPR, anche il futuro dei diritti fondamentali sembra passare attraverso l'adozione e lo sviluppo di queste nuove tecnologie.

In secondo luogo, i soggetti destinatari della regolazione comprendono fornitori di sistemi di AI, utilizzatori, distributori, importatori, sviluppatori di modelli di base nonché le autorità pubbliche competenti. In tal modo, la normativa si applica tanto ai grandi operatori multinazionali (come nella stagione caratterizzata dal DSA e DMA), quanto alle piccole e medie imprese e alle pubbliche amministrazioni che impiegano tali tecnologie (come nella stagione del GDPR). In altre parole, i destinatari sono, ad un tempo, definiti e indefiniti.

Su tali premesse, la regolazione prevista dall'AI Act deve rispondere alle esigenze previste nelle stagioni precedenti, associando rigore e flessibilità.

Ebbene, dall'analisi svolta in questo contributo, l'AI Act sembra contenere una regolazione che mira a coniugare queste due anime: da un lato, intende orientare l'evoluzione della società digitale europea in conformità agli obiettivi politici delineati dall'attore pubblico europeo, al fine di garantire uno sviluppo dell'intelligenza artificiale quanto più possibile affidabile, sicuro e coerente con i valori dell'Unione; dall'altro, è attribuito all'attore privato un ruolo altrettanto cruciale, in quanto chiamato a tradurre operativamente tali obiettivi attraverso la definizione di standard tecnici, procedure e autovalutazioni che assicurino la conformità dei sistemi di AI ai principi fissati dal legislatore, contribuendo così alla costruzione condivisa di un ecosistema regolatorio dinamico e flessibile.

Questa dinamica vede, quindi, una trasformazione della dimensione regolativa contemporanea: essa ambisce a combinare una

---

in *Agenda digitale*, 6 maggio 2025, disponibile su *https://www.agendadigitale.eu/mercati-digitali/dma-ue-allattacco-cosa-cambia-dopo-le-maxi-sanzioni-a-apple-e-meta/*.

co-regolazione più flessibile ad una più solida. In tale contesto, il concetto proprio di co-regolazione subisce una nuova modulazione.

Riprendendo il modello, illustrato in premessa, della co-regolazione concepita come una rete, la co-regolazione nella stagione dell'AI Act può essere intesa come una rete dinamica, capace di allargarsi o restringersi a seconda delle diverse esigenze. In questi termini, è possibile paragonarla ad una *sfera di Hoberman*, in quanto è capace di adattarsi e modulare la propria estensione in base alle necessità normative e ai contesti applicativi.

La *sfera di Hoberman*, secondo la scienza ingegneristica, è una sfera geodetica composta da una rete modulare i cui nodi e connessioni possono espandersi o restringersi a seconda degli impulsi esterni[70]. Trasponendo questo modello ideale alla regolazione prevista dall'AI Act, quando la sfera si apre le maglie si allargano, offrendo maggiore autonomia agli attori privati e stimolando l'innovazione, come avviene nella stesura di standard tecnici e nei processi di (auto)valutazione di conformità. Al contrario, quando la sfera si chiude le maglie si restringono, si consolidano gli obblighi e l'adesione agli stessi tramite la stesura di codici di condotta, esercitando, in tal modo, un controllo più rigoroso e garantendo la tutela degli interessi pubblici e dei diritti fondamentali.

La co-regolazione assume, così, una natura dinamica, capace di adattarsi sia al livello di rischio sia alla complessità del fenomeno da governare.

## 6. *Osservazioni conclusive*

A seguito della ricostruzione della co-regolazione nella società digitale svolta in questo contributo, è possibile formulare le seguenti riflessioni conclusive.

[70] La sfera di Hoberman è una struttura isocinetica brevettata nel 1990 da Chuck Hoberman, simile a una cupola geodetica, ma capace di ridursi fino a una frazione delle sue dimensioni originali grazie alle articolazioni snodabili che ne compongono la struttura. Il principio alla base del suo funzionamento è il cosiddetto meccanismo di Hoberman, un sistema dispiegabile che trasforma un movimento circonferenziale in un movimento radiale con un grado di libertà. Tale meccanismo può essere combinato per ottenere ulteriori gradi di libertà, rendendo la struttura altamente adat-

La regolazione della società digitale sembra aver raggiunto un nuovo orizzonte concettuale e operativo. In un contesto caratterizzato da fenomeni estremamente complessi e in rapido sviluppo, la norma intesa esclusivamente come strumento coattivo si rivela ormai insufficiente. La gestione efficace di tali fenomeni richiede un approccio *multi-attoriale*, in cui soggetti pubblici, attori privati e esperti di settore collaborano in maniera coordinata, con ruoli e responsabilità distinti ma complementari[71].

In tale prospettiva, si supera la dicotomia della co-regolazione a maglie larghe o a maglie strette delle stagioni precedenti: la co-regolazione nell'era dell'AI le contiene entrambe, riuscendo a combinarle sia nella predisposizione e nella stesura degli obblighi, sia nell'indurre gli operatori ad adottare tale regolazione, tramite l'adesione a codici di condotta, i quali diventano elemento essenziale per la *compliance* al Regolamento. Conseguentemente, sia il ruolo dell'attore pubblico che dell'attore privato è parimenti cruciale nella regolazione: il primo fissa gli obiettivi da perseguire e gli obblighi a cui attenersi; il secondo redige tecnicamente la natura degli stessi obblighi in modo da renderli modulabili con la realtà fortemente in trasformazione.

Per tale ragione, la regolazione nell'era dell'AI è assimilabile ad una *sfera di Hoberman*: un sistema dinamico e modulabile, capace di espandersi per includere nuovi attori e strumenti, o di contrarsi per esercitare un controllo più stringente in situazioni di rischio alto o sistemico. Tale metafora evidenzia la capacità della regolazione di adattarsi alla complessità dei fenomeni digitali senza perdere coerenza e integrità, bilanciando flessibilità e solidità.

---

tabile e modulabile. Per comprendere il funzionamento ingegneristico della sfera di Hoberman si rinvia a C. Hoberman, *Unfolding architecture*, in *Architectural design*, vol. 63, n. 3-4, 1993; V. Beatini, *Cinemorfismi. Meccanismi che definiscono lo spazio architettonico*, PhD Thesis in Forme e Strutture, 2011.

[71] D'altronde, la pervasività che la rete internet ha nel contesto sociale oggigiorno, non permette più una disciplina che sia solo affidata all'autoregolazione, come avvenuto nelle primissime fasi del fenomeno. Si prospetta, invece, una necessaria eteroregolazione, in cui sussista uno spazio di discussione utile a ricondurre la tecnica al bene della persona. Sul punto si rinvia a G. De Minico, *Libertà in Rete Libertà dalla Rete*, Giappichelli, Torino, 2020.

In tal modo, la co-regolazione nell'era dell'AI si configura come un ecosistema adattivo, in grado di modulare il proprio intervento in base al livello di rischio e alla complessità delle tecnologie coinvolte.

La normativa da sola non basta più: il futuro della governance digitale passa attraverso un equilibrio tra politica, competenza tecnica e partecipazione dei privati, un modello che, come la *sfera di Hoberman*, sa espandersi e contrarsi senza perdere integrità, rappresentando un paradigma replicabile anche in altri settori altamente innovativi.

L'approccio adattivo della regolazione della società digitale emerso dall'analisi svolta in questo contributo, viene maggiormente manifestato dall'ultimo pacchetto normativo proposto dalla Commissione europea.

Il 19 novembre 2025 è stato pubblicato il c.d. *Digital Omnibus*, una proposta di regolamento che mira ad armonizzare e coordinare il quadro normativo digitale europeo. Esso si compone di tre diverse proposte di regolamento: la prima, COM(2025) 835, proposta sulla *Data Union Strategy*; la seconda, COM(2025) 836, proposta di semplificazione e revisione dell'AI Act; infine, la terza, COM(2025) 837, proposta sul *digital acquis*[72].

Per quanto riguarda il focus di questo contributo, la COM (2025) 836, si inserisce nel quadro della regolazione adattiva e modulabile, come raffigurato dalla metafora della *sfera di Hoberman*. Infatti, è prevista una semplificazione delle regole, come indicato, ad esempio, dal nuovo art. 43, par. 3, che dispone l'unificazione delle procedure di valutazione di conformità, laddove gli organismi notificati potranno valutare la conformità di sistemi ad alto rischio, rinunciando alla «valutazione di terze parti, a condizione che abbia(no) applicato norme armonizzate che coprono tutti i requisiti pertinenti». In altri termini, si permette al fabbricante di valutare esso stesso, qualora in linea con i requisiti previsti dal regolamento, la conformità del sistema di AI ad alto rischio, senza richiedere altre valutazioni di conformità.

[72] Si rinvia a Commissione europea, *Proposta di regolamento omnibus digitale*, consultabile al link: *https://digital-strategy.ec.europa.eu/it/library/digital-omnibus-regulation-proposal*.

Ancora, si estende la semplificazione delle regole, già previste per le PMI, alle small mid-caps (SMCs), l'alfabetizzazione dell'AI passa da un dovere in capo agli operatori di sistemi di AI ad un dovere in capo agli Stati membri e alla Commissione (art. 4). Inoltre, è previsto un ampio spazio per la sperimentazione delle nuove tecnologie di AI, istituendo un sandbox europeo, con un approccio real-world (art. 60a).

A tale maggiore flessibilità della regolazione ne corrisponde, però, un deciso accentramento dei poteri di sorveglianza e controllo in capo alla Commissione, ovvero all'AI Office. Il nuovo art. 75 afferma che l'AI Office è «esclusivamente competente per la vigilanza e l'applicazione del presente regolamento a tali sistemi» (ovvero sistemi di AI per finalità generali, GPAI). L'art. in questione continua affermando che «l'AI Office è altresì esclusivamente competente per la vigilanza e l'applicazione degli obblighi previsti dal presente regolamento nei confronti di sistemi di AI che costituiscono o sono integrati in piattaforme online di grandi dimensioni o motori di ricerca di grandi dimensioni, ai sensi del Reg. UE 2022/2065 (DSA)». In tale prospettiva, l'AI Office detiene tutti i poteri di sorveglianza del mercato, come previsto dal Reg. UE 2019/1020, tra cui anche il potere di imporre sanzioni (art. 75, par. 1, lett. *a*). Inoltre, spetta alla Commissione, ai sensi della nuova formulazione dall'art. 75, par. 1, lett. *c*, effettuare valutazioni di conformità pre-market per i sistemi di AI per finalità generali che siano classificati ad alto rischio e soggetti a valutazione di conformità da terze parti ai sensi dell'art. 43, prima che tali sistemi siano immessi sul mercato. I costi di questa valutazione sono addebitati agli operatori di sistemi di AI.

Dall'analisi di queste possibili modifiche all'AI Act emerge una tendenza alla centralizzazione delle competenze, affidate alla Commissione e all'AI Office per quanto riguarda i sistemi GPAI, in particolare quelli delle grandi piattaforme digitali, al fine di garantire il coordinamento tra le disposizioni dell'AI Act e quelle del DSA.

In altri termini, sembra delinearsi un restringimento delle maglie della regolazione: come già avvenuto nella stagione del *Digital Package*, quando le tecnologie di intelligenza artificiale sono integrate nelle grandi piattaforme digitali, si assiste a una centralizzazione del potere di vigilanza e controllo in capo alla Commissione.

A questo, ne segue una semplificazione, e quindi una maggiore flessibilità, delle regole per le imprese di dimensioni ridotte o medie (SMCs), con minore liquidità sul mercato azionario.

Ne risulta, dunque, una regolazione più flessibile e adattiva per le imprese di piccole e medie dimensioni, che invece si fa più rigorosa – con un ruolo di vigilanza centrale attribuito all'AI Office e alla Commissione – quando riguarda le grandi piattaforme digitali.

Sembra, dunque, che la Commissione europea, con questa proposta di regolamento, intenda da un lato favorire lo sviluppo delle imprese SMCs (maggiormente presenti nel tessuto economico europeo)[73] nel settore dell'AI, attraverso un quadro normativo più flessibile, e dall'altro esercitare una vigilanza e un controllo più stringenti sulle grandi piattaforme digitali (di matrice soprattutto statunitense) che, come evidenziato nell'analisi del *Digital Package*, rappresentano un rischio significativo sia per la concorrenza di mercato sia per gli equilibri democratici.

In conclusione, dalla lettura di questa proposta di regolamento, si può ritenere che questa rifletta una più ampia strategia di tutela degli interessi europei nel contesto della competizione globale per il controllo delle nuove tecnologie di AI. Essa sembra infatti orientata a rafforzare l'autonomia regolatoria dell'Unione di fronte alla presenza delle grandi piattaforme digitali, perlopiù extraeuropee, che detengono un potere economico e tecnologico tale da incidere sugli equilibri del mercato interno e, in ultima analisi, sull'indipendenza strategica dell'Europa nel settore digitale.

[73] Il settore economico europeo è basato sulla presenza di PMI e SMCs, mentre è relativamente inferiore la presenza di grandi Big companies. Sul punto si veda Stoxx, *Under the Spotlight: A closer look at European equities*, consultabile al link: *https://stoxx.com/under-the-spotlight-a-closer-look-at-european-equities/#:~:text=European%20equities%20are%20having%20a,EUR%208.5%20billion%20in%202022*.

FULVIA ABBONDANTE

# PRIME PROVE DI SOVRANITÀ DIGITALE: LA REGOLAMENTAZIONE DELLE TELECOMUNICAZIONI E LA PROTEZIONE DEI DATI PERSONALI NEL REGNO UNITO POST-BREXIT



## 1. *La regolamentazione delle telecomunicazioni nel Regno Unito: una breve introduzione*

### 1.1. *Dalla liberalizzazione alla separazione funzionale di BT*

La disciplina delle telecomunicazioni (d'ora innanzi tlc) nel Regno Unito presenta una traiettoria che anticipa, in larga misura, i successivi sviluppi europei. La Gran Bretagna è stata, infatti, tra i primi Paesi in Europa a privatizzare il proprio operatore nazionale e ad aprire il mercato alla concorrenza, avviando un processo di riforma già a metà degli anni Ottanta del Novecento e sviluppandolo lungo un percorso che è stato influenzato sia dall'esperienza statunitense sia da quella giapponese, ordinamenti considerati, all'epoca, i più avanzati nella trasformazione del settore. Il *Telecommunications Act* 1984[1] avviò il processo di privatizzazione di British

[1] *Telecommunication Act* 1984, in *https://www.legislation.gov.uk/ukpga/1984*.

Telecom (d'ora innanzi BT), mediante la vendita iniziale del 51% del capitale, cui seguì, con il *Duopoly Review* del 1993, la cessione della totalità delle azioni BT che venne privatizzata come impresa verticalmente integrata, responsabile tanto delle infrastrutture quanto dei servizi. Consapevole del rischio di fallimenti di mercato, il legislatore inglese istituì contestualmente l'*Office of Telecommunication* (d'ora innanzi Oftel) Autorità settoriale incaricata di monitorare l'adempimento delle licenze rilasciate dal Governo e di garantire il rispetto delle condizioni concorrenziali. La configurazione duopolistica composta da BT e dal nuovo entrante Mercury si rivelò tuttavia insufficiente a garantire un effettivo equilibrio competitivo né tantomeno un adeguato livello di tutela dei consumatori[2].

Soltanto nel 2003 – anche grazie all'impulso derivante dal riordino del quadro europeo delle comunicazioni elettroniche – il Regno Unito conobbe una trasformazione radicale del settore, con l'adozione del *Communication Act* 2003[3] che in adempimento del pacchetto Direttive del 2002[4] istituì una nuova Autorità di regolazione l'Ofcom[5], che venne dotata sia di poteri *ex ante* di regolazione settoriale sia di competenze *ex post* di matrice antitrust, provenienti dal *Competition Act* 1998 e *dall'Enterprise Act* 2002[6]. La logica sottesa alla politica di *regulation* britannica era chiara: nei mercati delle tlc caratterizzati da lunghi anni di presenza di un monopolista e al massimo di altro operatore la concorrenza non poteva essere

---

[2] Sul punto P.W.J. De Bijl, M. Peitz, *Regulation and Entry into Telecommunications Markets*, Cambridge 2002; A. La Spina, G. Maione, *Lo Stato regolatore*, Bologna, 2000.

[3] *Communication Act* 2003 in *https://www.legislation.gov.uk/ukpga/2003/21/contents*.

[4] Per un ampio commento sulla regolazione europea e sul suo impatto anche in UK si v G. De Minico, *Le Direttive CE sulle comunicazioni elettroniche dal 2002 alla revisione del 2006. Un punto fermo?*, in *www.forumcostituzionale*, e relativamente sia al pacchetto direttive 2002 sia la successiva modifica intervenuta ne 2009 si v. della stessa A. *Internet Regola Anarchia*, Napoli, 2012, e specificamente 53-57.

[5] *Office of Communication* (Ofcom), istituita dall'*Office of Communications Act* 2002, in *https://www.legislation.gov.uk/ukpga/2002/11/contents* ed operativa dal 2003, con competenze allargate rispetto all'Oftel, comprendenti telecomunicazioni, radiodiffusione e servizi postali.

[6] *Enterprise Act* 2002, *https://www.legislation.gov.uk/primary+secondary?title=Enterprise%20Act%202002&sort=*.

raggiunta grazie al funzionamento spontaneo del mercato e, dunque, l'unica possibile soluzione per favorire nuovi entranti era l'introduzione di norme *ex ante* per limitare il potere dell'*incumbent* e favorire l'emergere di una competizione effettiva.

Già all'atto del suo insediamento (nel dicembre 2003) l'Ofcom avviò *Strategic Telecommunications Review*[7] una consultazione pubblica di ampio respiro volta ad accertare se il settore generasse benefici per gli utenti finali e quale fosse l'impatto dei diversi approcci regolatori possibili. Al termine dell'istruttoria, l'autorità concluse che il mercato presentava ancora significative strozzature strutturali, imputabili alla posizione di British Telecom (BT), che continuava a detenere un Significativo potere di Mercato (d'ora innanzi SMP) in 14 mercati all'ingrosso e 16 al dettaglio.

L'*unbundling*, imposto a BT, si dimostrò scarsamente efficace: troppo oneroso, tecnicamente arretrato e non idoneo a sostenere un modello effettivamente concorrenziale. La conseguenza fu che non si sviluppò una competizione basata sull'accesso disaggregato alla rete. Gli stakeholder denunciarono, altresì, la capacità dell'*incumbent* di favorire le proprie divisioni interne, pregiudicando gli operatori terzi nei mercati *downstream*.

Alla luce di tali criticità, l'Ofcom ritenne necessario introdurre rimedi asimmetrici *ex ante* per garantire una «piena parità di accesso». Per evitare misure più invasive ai sensi dell'*Enterprise Act* del 2002, nel 2004, BT propose all'autorità un articolato sistema di impegni volontari (*Undertakings*), anche al fine di evitare una separazione proprietaria, accettati dall'*Ofcom* ed entrati in vigore il 22 settembre 2005[8].

Gli *Undertakings* perseguivano l'obiettivo dell'*Equality of Access* attraverso due strumenti fondamentali, l'*Equivalence of inputs* ossia la fornitura agli operatori alternativi degli stessi prodotti e con le stesse condizioni garantite alle divisioni interne di BT e separa-

---

[7] OFCOM, *Strategic Review of Telecommunications* del 3 February 2005, in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/uncategorised/8789-telecoms_p2/statement/annexes/maincondoc.pdf?v=332682*.

[8] OFCOM, *Final statements on the Strategic Review of Telecommunications, and undertakings in lieu of a reference under the Enterprise Act* 2002, in *https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/statement_tsr*.

zione funzionale, con la creazione di Openreach quale entità distinta ma pur sempre collegata a BT incaricata di gestire i prodotti di accesso.

La governance venne profondamente riorganizzata: fu istituito *l'Equivalence of Access Board*, affiancato dal*l'Equivalence of Access Office*, e furono introdotti sistemi di incentivazione che vietavano *bonus* legati ai risultati complessivi di BT Group, legandoli esclusivamente agli obiettivi di Openreach[9].

Dopo dodici anni di vigenza degli *Undertakings* del 2005 e la rapida evoluzione delle tecnologie delle tlc, nonché il tumultuoso sviluppo della rete e delle connesse tecnologie digitali, impose una revisione della politica regolatoria dell'Autorità Indipendente, anche per i numerosi interventi del Governo Inglese che miravano a creare un mercato digitale e, dunque, competitivo e volto a favorire la connessione a banda larga e ultralarga, una rete che garantiva agli utenti la possibilità di ottenere tutti i servizi di nuova generazione.

La *Digital Communications Review* dell'Ofcom rilevò che la separazione funzionale non era riuscita a neutralizzare la capacità di BT di essere un operatore verticalmente integrato in grado di avere ancora un SPM in ampie zone del Regno Unito. Nonostante l'accesso di nuovi operatori di rete non si era sviluppato un mercato effettivamente competitivo[10] e nella nuova fase di transizione alla fibra era necessario intervenire nuovamente per evitare che anche nel mercato di questa nuova tecnologia venissero a crearsi strozzature.

Dal 2012 al 2017 anche i Governi del Regno Unito avviarono politiche regolatorie che favorissero sia lo sviluppo delle nuove infrastrutture di rete, in particolare la fibra, e della rete *wirless* e l'utilizzazione della telefonia cellulare quale alternativa ai *bottlencks* permanere sulla linea fissa, anche in presenza di una regolazione *ex ante* e gli impegni sottoscritti da BT di realizzare un mercato effettivamente competitivo.

---

[9] Sul punto ci si permette rinviare a F. Abbondante, *L'ordinamento delle telecomunicazioni in Gran Bretagna fra continuità e discontinuità*, in P. Costanzo, G. De Minico, R. Zaccaria, *I tre codici della Società dell'informazione*, Torino, 2006, specificamente 230-231.

[10] Ofcom, *Digital Communications Review*, 11 March 2015, in *https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/digital-comms-review*.

Nel marzo 2017 BT presentò, e l'Ofcom accettò, un ulteriore impegno volontario di riforma per evitare la separazione proprietaria, Openreach è divenuta una società distinta (*Openreach Limited*), dotata di un proprio Consiglio di amministrazione, con maggioranza indipendente dal gruppo BT, personale e strategia autonomi. La separazione non è stata tuttavia strutturale o proprietaria, bensì una *legal separation* più profonda e articolata[11]. Una parte della dottrina ha osservato che neppure tale modello garantiva la neutralità necessaria per favorire co-investimenti effettivamente competitivi, specie nel mercato della fibra, suggerendo l'esigenza – ancora attuale – di valutare forme di separazione più incisive sebbene vi sia un acceso dibattito se tale estrema misura è o meno consentita all'Autorità di settore nel silenzio di un'espressa previsione del *Communication Act* del 2003[12].

Parallelamente alla riforma della governance di BT/Openreach, il legislatore britannico è intervenuto con una serie di politiche regolatorie, mediante la *UK Digital Strategy* 2017, che delineava una *roadmap* orientata al completamento della copertura 4G e della banda larga superveloce entro il 2020, all'introduzione di un *Universal Service Obligation* (d'ora innanzi USO), allo sviluppo del 5G e a ingenti investimenti nelle infrastrutture digitali di nuova generazione. La strategia prevedeva altresì programmi nazionali di alfabetizzazione digitale, un quadro regolatorio favorevole all'innovazione, iniziative nel settore dell'intelligenza artificiale e misure finalizzate alla sicurezza cibernetica[13].

Nello stesso anno, il Parlamento ha approvato il *Digital Economy Act* 2017[14] un piano strategico che, tenendo in considerazione

---

[11] Ofcom, *Delivering a more independent Openreach*, Statement published 13 July 2017, in *https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/delivering-a-more-independent-openreach*.

[12] J. Whalley, P. Curwen, *Is Functional Separation BT-Style the Answer?*, in *Communications & Strategies*, n. 70, 2008; R. Cadman, *Legal separation of BT: A necessary incentive for investment?*, in *Teleccomuncation policy*, Volume 43, Issue 1, February 2019, Pages 38-49.

[13] Department for Science, Innovation& Technology, Department for Digital, Culture, Media & Sport, *UK Digital Strategy 2017*, in *https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy*.

[14] *Digital Economy Act* 2017, in *https://www.legislation.gov.uk/ukpga/2017/30/contents*.

le profonde trasformazioni intervenute, potesse incentivare la realizzazione di infrastrutture e sui servizi di comunicazioni. In particolare, il Regno Unito è stato il primo paese nel contesto europeo ad introdurre un USO di connettività *broadband* (10 Mbps), da attuare nel 2018 con la designazione di BT e KCOM come fornitori universali. Nel medesimo tempo sono state previste norme sulla condivisione dei dati tra amministrazioni. In considerazione dell'ampia diffusione di contenuti lesivi per i minori venne introdotto un regime di verifica dell'età per i contenuti pornografici e filtri per contenuti per adulti. In ragione dell'aumentata complessità del mercato delle tlc vennero introdotti maggiori poteri sanzionatori per l'Ofcom e modifiche all'*Electronic Communications Code* per facilitare l'installazione di infrastrutture. Inoltre, vengono introdotti aumenti delle pene per violazioni del *copyright online*; attribuzione all'Ofcom del ruolo di regolatore esterno della BBC.

In questo contesto si innesta l'imprevisto e, per certi versi imprevedibile, processo di separazione dall'UE che, avviato dopo il referendum del 2016, si è concluso il 31 gennaio 2020, data di uscita del Regno Unito dall'Unione Europea. Un divorzio lungo e complesso che si è realizzato in più fasi e scandito da numerosi accordi fra le due parti per consentire una transizione il meno dolorosa possibile.

Con il definitivo abbandono del contesto unionale con il Regno Unito ha dovuto provvedere all'adeguamento della normativa interna che per gran parte derivava da quella sovranazionale.

Nella fase transitoria di uscita dalla UE e il ritorno ad una piena sovranità legislativa alcuni atti, molti dei quali mantengono nella sostanza la regolazione europea, sono appunto oramai norme interne a pieno titolo. Tra di esse vanno menzionate – gli *Electronic Communications and Wireless Telegraphy (Amendment etc.) (EU Exit) Regulations* 2019[15]; i *Broadcasting (Amendment) (EU Exit) Regulations* 2019[16]; i regolamenti del 2020 che hanno recepito la direttiva (UE) 2018/1972, *European Electronic Communications Code*

[15] *The Electronic Communications and Wireless Telegraphy (Amendment etc.) (EU Exit) Regulations* 2019, in *https://www.legislation.gov.uk/uksi/2019/246/made*.

[16] *The Broadcasting (Amendment) (EU Exit) Regulations* 2019, in *https://www.legislation.gov.uk/uksi/2019/224/contents*.

(EECC)[17]. Successivamente, ulteriori atti hanno completato la riallocazione delle competenze normative il *Telecommunications (Security) Act* 2021[18], che ha rafforzato gli obblighi di sicurezza e attribuito al Governo poteri di interdizione per ragioni di sicurezza nazionale; – il *National Security and Investment Act* 2021[19], che ha riformato il controllo delle acquisizioni nei settori critici – il *Product Security and Telecommunications Infrastructure Act* 2022[20], che ha modificato in modo significativo l'*Electronic Communications Code*, facilitando l'installazione di infrastrutture di rete e introducendo rigidi standard di sicurezza per i prodotti digitali post-Brexit. Pur sostituendo il precedente quadro europeo, il sistema britannico è rimasto in larga parte compatibile con lo schema preesistente, mantenendo un'impostazione fondata sull'accesso regolato e sull'individuazione di SMP.

### 1.2. *La nuova stagione regolatoria: fibre networks, nuovi rimedi e servizi satellitari* direct-to-device

Con l'avvio del processo di definitiva uscita dall'Unione Europea il Regno Unito ha intrapreso un percorso di progressiva riscrittura della propria *regulation* sebbene parte di quella europea sia ancora in vigore in quanto trasfuse nell'ordinamento interno, ma che possono essere modificate unilateralmente senza incorrere in sanzioni da parte della Commissione Europea, pur dovendo tenere conto dei riflessi sul commercio e sugli scambi.

Il divorzio dalla UE non ha modificato sostanzialmente il mercato del UK delle tlc che ha continuato ad essere caratterizzato da una limitata concorrenza sulla linea fissa, a causa della presenza di BT come operatore verticalmente integrato, che ha impedito, almeno fino ad oggi, un non adeguato sviluppo della fibra nonostante

---

[17] *The Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations* 2020, in *https://www.legislation.gov.uk/uksi/2020/1419/contents*.

[18] *Telecommunications (Security) Act* 2021, in *https://www.legislation.gov.uk/ukpga/2021/31*.

[19] *National Security and Investment Act* 2021, in *https://www.legislation.gov.uk/ukpga/2021/25/contents*.

[20] *Product Security and Telecommunications Infrastructure Act* 2022, in *https://www.legislation.gov.uk/primary+secondary?title=Product%20Security%20and%20Telecommunications%20Infrastructure%20Act%20*.

la normativa asimmetrica introdotta dall'Autorità di settore e la separazione legale dell'*ex incumbent*. A fronte di queste difficoltà nel mercato della *fixed line* molto dinamico è, invece, il mercato del mobile dove si è realizzata un'effettiva competizione.

In questo contesto si colloca la recente consultazione avviata da Ofcom, *Promoting competition and investment in fibre networks: Telecoms Access Review 2026-31*[21], che ha lo scopo di valutare il contesto strategico delle proposte e la loro conformità agli obblighi giuridici, nonché le decisioni in materia di definizione del mercato, accertamento del SMP e relativi rimedi da applicare a BT quale operatore verticalmente integrato. L'obiettivo è quello di favorire la competizione senza tuttavia disincentivare gli investimenti che BT ha intrapreso per la transizione dalla rete in rame alla fibra ottica ultraveloce.

Più precisamente e analiticamente, dunque, l'Ofcom propone il mantenimento dell'accesso alle infrastrutture di Openreach (pali telegrafici e condotti sotterranei), imponendo all'operatore l'obbligo di consentire agli altri *providers* di installare e gestire le proprie reti in fibra attraverso i prodotti di *Physical Infrastructure Access* (PIA). Tale accesso è accompagnato da un rigoroso obbligo di non discriminazione indebita e da tariffe basate sui costi effettivi, in modo che i canoni riflettano la restituzione di una quota equa delle spese sostenute da Openreach in proporzione all'utilizzo dell'infrastruttura[22].

Si conferma, inoltre, un approccio differenziato alla regolamentazione della banda larga all'ingrosso in base alle condizioni concorrenziali delle diverse aree del Regno Unito. L'Ofcom ha pro-

---

[21] Ofcom, *Promoting competition and investment in fibre networks: Telecoms Access Review 2026-31*, in *https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/consultation-promoting-competition-and-investment-in-fibre-networks-telecoms-access-review-2026-31*. Tale documento era stato preceduto da Ofcom, *Statement: Promoting investment and competition in fibre networks - Wholesale Fixed Telecoms Market Review* 2021-26, in *https://www.ofcom.org.uk/phones-and-broadband/telecoms-infrastructure/2021-26-wholesale-fixed-telecoms-market-review*.

[22] In particolare si v. Ofcom, *Promoting competition and investment in fibre networks: Telecoms Access Review 2026-31 Volume 3: Non-Pricing Remedies*, in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-telecoms-access-review-2026-31/main-documents/volume-3-non-pricing-remedies.pdf?v=392946*, specificamente 13-17.

posto, infatti una ripartizione in zone che presentano differenti gradi di *competition*.

Un'Area 1, caratterizzata dalla presenza stabile di almeno due operatori non verticalmente integrati, nella quale non si ritiene necessario mantenere una regolazione stringente. Un'Area 2, che copre la parte maggioritaria del territorio, nella quale la concorrenza è in via di consolidamento: qui l'Autorità intende fissare prezzi stabili – indicizzati all'inflazione per i prodotti di banda larga superveloce «base», consentendo maggiore flessibilità sui servizi di fascia superiore e spostando la regolazione di *price cap* dai prodotti fino a 40 Mbit/s a quelli fino a 80 Mbit/s, in linea con l'evoluzione dei consumi di dati. Un'Area 3, pari a circa il 10% del territorio, in cui non esiste e difficilmente potrà esistere un potenziale per una concorrenza significativa e sostenibile. In tali aree si mira a consentire a Openreach il recupero dei costi ragionevoli degli investimenti nella rete *full-fiber*, riconoscendo al tempo stesso il ruolo decisivo dei sussidi pubblici e promuovendo la concorrenza basata sull'accesso alla rete[23].

A quest'ultima è preclusa la facoltà di praticare sconti geografici e l'Ofcom intende estendere tale restrizione a tutte le tariffe (non limitandola ai soli canoni di affitto come nella revisione precedente). Qualora Openreach intenda modificare le tariffe, deve notificare l'intenzione di introdurre determinate condizioni commerciali con un preavviso di 120 giorni, consentendo all'Autorità di valutare le eventuali offerte prima della loro entrata in vigore. L'Ofcom sta predisponendo linee guida aggiornate sui tipi di offerte commerciali che potrebbero essere considerate problematiche.

I rimedi previsti devono essere progressivamente trasferiti (incluse le protezioni tariffarie) dai servizi in rame a quelli in fibra completa, in conformità all'approccio delineato nel 2021. Openreach, secondo l'impostazione dell'Autorità di settore, avvierà la dismissione delle centrali durante il periodo di revisione, negoziando attualmente con i propri clienti i termini specifici del passaggio dal rame

[23] Sul punto OFCOM P*romoting competition and investment in fibre networks: Telecoms Access Review 2026-31*, Volume 4: *Pricing Remedies* in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-telecoms-access-review-2026-31/main-documents/volume-4-pricing-remedies.pdf?v=392947*, 5-7.

alla fibra. L'Ofcom intende sostenere gli obiettivi di Openreach, che offrono l'opportunità anche per altri fornitori di consolidare l'infrastruttura, ridurre il consumo energetico e incrementare l'efficienza.

Per quanto riguarda l'approccio alla regolamentazione delle linee affittate in diverse parti del Regno Unito, per il livello attuale o potenziale di concorrenza esistenti, devono essere considerate le condizioni competitive variabili nel Regno Unito per la fornitura di servizi. In questo mercato vanno dunque applicate regole diverse rispetto ai servizi *broadband* all'ingrosso, che riflettano le differenze nello sviluppo dei mercati dal 2021. Per quanto riguarda l'Area Centrale di Londra essa è stata deregolamentata dal 2019 e non si prevedono cambiamenti al momento.

Pe le altre aree geografiche Ofcom propone, anche in questo caso, un criterio differenziato a seconda del grado di concorrenza raggiunta.

Nell'area a denominata ad alta copertura di rete (*High Network Reach* - HNR) dove c'è una concorrenza significativamente maggiore nelle reti di linee affittate, ma BT ha ancora SMP, il rimedio proposto da Ofcom è che quest'ultima debba fornire accesso ai suoi servizi di linee affittate a prezzi equi e ragionevoli.

Nell'Area 2 dove c'è, o è probabile che ci sia, il potenziale per una concorrenza materiale e sostenibile, che copre il 42% del Regno Unito, *Openreach* dovrebbe fornire accesso ai suoi servizi attivi di linee affittate e di fissare tetti di prezzo fissi, adeguati all'inflazione.

Nell'Area 3, che copre il 46% del Regno Unito, dove non c'è, e non è probabile che ci sia, il potenziale per una concorrenza materiale e sostenibile, Ofcom propone di fornire fibra spenta (ci sono i cavi ma non la connessione) e di fissare i prezzi in base a costi ragionevole fornendo accesso ai suoi servizi attivi di linee affittate. Per i servizi attivi a larghezza di banda più elevata (maggiore di un 1GB), il regolatore ritiene di mantenere tetti di prezzo fissi, adeguati all'inflazione, mentre il mercato transita verso la fibra spenta. Per i servizi attivi a larghezza di banda inferiore l'Autorità di settore ha introdotto limiti stringenti agli sconti geografici praticabili da Openreach, prevedendo l'obbligo di notificare con 120 giorni di anticipo l'introduzione di determinate condizioni commerciali, così da consentire all'Autorità di settore una valutazione *ex ante* delle

offerte e valutare se esse possano essere potenzialmente distorsive delle concorrenze.

Un ulteriore profilo riguarda il supporto alla migrazione dalle reti *legacy* e la dismissione delle centrali: i rimedi regolatori – incluse le protezioni sui prezzi – dovranno progressivamente transitare dai servizi in rame a quelli in fibra completa, favorendo la razionalizzazione dell'infrastruttura, la riduzione dei consumi energetici e l'efficienza complessiva del sistema[24].

Di particolare interesse è, infine, l'attenzione rivolta all'espansione della connettività tramite satelliti non geostazionari e servizi di comunicazione *device-to-device* (D2D) e satellite *direct-to-device* (SD2D). La comunicazione D2D consente ai dispositivi di dialogare direttamente, senza passare per la rete cellulare centrale, risultando utile in contesti di scarsa copertura o per lo scambio rapido di dati in prossimità, ampliando la copertura in aree prive di celle terrestri e offrendo un canale di *backup* in caso di guasto della rete. In entrambi i casi, le tecnologie summenzionate offrono vantaggi significativi per la comunicazione e la connettività, sia in situazioni di emergenza che per l'efficienza delle reti cellulari e potrebbe rappresentare una tecnologia in grado di superare il *digital divide*. Per tale ragione, l'Ofcom ha pubblicato nel settembre 2025 uno *Statement*, che fa seguito ad una consultazione pubblica avviata nel marzo di quest'anno, e ha deciso di introdurre un quadro autorizzatorio per i servizi *direct-to-device* (D2D).

Da questo punto di vista il Regno Unito si colloca tra le prime giurisdizioni europee a normare in modo organico la convergenza tra reti terrestri e satellitari. Tale scelta si fonda su un'esigenza di politica regolatoria dinamica: garantire connettività universale e resilienza delle reti, anticipando l'evoluzione tecnologica e senza attendere gli esiti di ulteriori determinazioni da parte degli enti regolatori internazionali. La *ratio* dell'intervento è duplice: sanare le asimmetrie territoriali fra zone servite e aree totalmente sfornite di copertura di rete,

[24] OFCOM, *Promoting competition and investment in fibre networks: Telecoms Access Review 2026-31 Volume 1: Overview, summary and structure*, in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/consultation-telecoms-access-review-2026-31/main-documents/volume-1-overview-summary-and-structure.pdf?v=392944*, 5-7.

fornire livello ulteriore di capacità di reazione alle infrastrutture critiche, soprattutto in caso di guasti alle reti terrestri. Questo orientamento si colloca nel solco della tradizione britannica di regolazione anticipatoria delle telecomunicazioni, già osservata nella riforma del 2002 con la creazione di Ofcom e, prima ancora, nell'esperienza pionieristica di Oftel. Il punto più rilevante della decisione di Ofcom consiste nell'obbligo per gli operatori di rete mobile (MNO) di richiedere una variazione delle licenze di accesso allo spettro già detenute. In base al WTA 2006, ogni mutamento della licenza deve essere conforme ai principi di uso efficiente dello spettro, non interferenza dannosa tutela dei servizi essenziali.

La scelta di intervenire mediante *licence variation*, anziché attraverso nuove assegnazioni, comporta due conseguenze: continuità regolatoria per gli operatori, che mantengono le loro bande ma le estendono a usi non terrestri; evitare nuove gare di spettro, circostanza che avrebbe rallentato l'introduzione della tecnologia e creato tensioni sul mercato. L'Autorità Indipendente ha introdotto anche nuovi regolamenti di esenzione (*exemption regulations*), che permettono ai dispositivi degli utenti finali di connettersi ai satelliti senza richiedere una licenza individuale. Questa soluzione ricalca la logica già adottata con i dispositivi Wi-Fi e ad uso personale: la licenza grava sull'operatore, non sull'utente. In tal modo si ha una riduzione degli oneri amministrativi, in linea con l'approccio *light-touch* storicamente adottato dal regolatore; la piena legittimazione dell'utente a utilizzare il servizio senza rischi di violazione del WTA del 2006. Una parte significativa del documento è dedicata ai rischi di interferenza e di protezione dei radar dell'aviazione civile nella banda 2,6 GHz.

Le condizioni tecniche proposte includono: limiti specifici di potenza EIRP per i satelliti; profili di emissione controllati; obblighi di coordinamento internazionale; misure anti-interferenza e protezioni aggiuntive per i servizi aeronautici. Ofcom adotta qui un approccio di *risk-based regulation*, idoneo a bilanciare innovazione e tutela della sicurezza[25].

[25] OFCOM, *Enabling satellite direct to device services in mobile spectrum bands*, 17 november 2025, in *https://www.ofcom.org.uk/spectrum/space-and-satellites/consultationenabling-satellite-direct-to-device-services-in-mobile-spectrum-bands*.

Vi è da dire che l'Autorità di settore ha già, in passato, autorizzato operatori come *Starlink* e *Amazon* a fornire servizi di accesso a banda larga ad alta velocità e bassa latenza tramite terminali dedicati, senza tuttavia indire nuove aste di frequenze né istituire procedure autorizzative *ad hoc* per i *gateway* satellitari, affidandosi ai meccanismi di mercato esistenti[26]. Il Governo ha stanziato risorse significative per progetti satellitari e per lo sviluppo di *chip* compatibili con le tecnologie emergenti, ponendo questioni non marginali di sovranità digitale, in quanto due grandi operatori statunitensi hanno acquisito una presenza strutturale sul territorio britannico[27].

In entrambe i casi vi sono nuove e significative sfide che interesseranno i regolatori non solo europei. In primo luogo, la normazione degli spazi non terrestri già ampiamente occupati dai pionieri del satellitare. In secondo luogo, la regolazione dei dati che ancor più che in passato verranno trasferiti fuori non solo da contesti territoriali del globo terrestre ma addirittura al di fuori di essi.

### 1.3. *Il principio della Net Neutrality pre e post Brexit in Uk*

Il principio della *Net Neutrality*, com'è noto, è stato oggetto di un ampio dibattito ambito europeo. Nato nel contesto americano come regola tecnica e anti-discriminatoria a presidio della *fair competition* fra operatori fornendo, a parità di condizioni la stessa velocità di banda, ha consentito lo sviluppo e l'innovazione di servizi e contenuti. Nel contesto europeo il rispetto della neutralità della rete è stato indissolubilmente legato alla libertà d'uso di Internet e alla tutela dei diritti fondamentali. La vorticosa e rapidissima tra-

---

[26] OFCOM, *Statement: Decision to grant temporary licences to Starlink Services LLC to use 71-76 GHz and 81-86 GHz for NGSO gateway earth stations at three sites*, 28 October 2025, in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/consultation-temporary-ngso-gateway-access-to-e-band/statement-temporary-ngso-gateway-access-to-e-band.pdf?v=406905*; ID., *Ofcom grants NGSO licence to Amazon Kuiper and releases spectrum to boost connectivity*, *https://www.ofcom.org.uk/spectrum/space-and-satellites/statement-amazon-kuiper-services-europe-sarl-application-for-a-non-geostationary-earth-station-network-licence?*.

[27] *UK backs next-generation satellite communications with £ 6.9 million investment*, Press release, 21 November 2025, in *https://www.gov.uk/government/news/uk-backs-next-generation-satellite-communications-with-69-million-investment*.

sformazione tecnologica ha evidenziato l'inadeguatezza della *Net Neutrality* come strumento a garanzia della concorrenza e, con il passaggio al *multi sided market* nel quale l'utilizzatore finale non solo assume un ruolo fondamentale ma esercita la libertà di informazione, che si affianca a quella esercitata nel mondo *offline*. Attribuire al fornitore di accesso la possibilità di scegliere a quale contenuto o servizio dare priorità finisce per produrre effetti negativi anche sull'utente finale; quest'ultimo, infatti, potrà scegliere solo quello che gli verrà proposto da chi è in grado di sopportare un costo maggiore per ottenere una linea più veloce.

La *Net Neutrality* tutelando la possibilità di accedere indistintamente a tutti i contenuti da parte degli *end users* non è più e non solo lo strumento per garantire la libera concorrenza fra fornitori di servizi e contenuti ma mezzo per assicurare un valore ben più rilevante quale quello della *freedom of information*[28]. Un principio applicato in origini in via di prassi [29] che però ha trovato una sua consacrazione regolatoria nei primi decenni degli anni Duemila sia negli USA[30] sia nella UE. Il Regolamento Europeo n. 2015/2120[31] dopo aver affermato il divieto di bloccare, limitare il traffico o addebitare tariffe suppletive introduceva una serie di deroghe importanti relati-

---

[28] Cfr. G. De Minico, *Net neutrality come diritto fondamentale di chi verrà*, in *Costituzionlimo.it*, 1/2016, 7.

[29] La neutralità della Rete è stata anche definita all'art. 4 nel primo documento, che pur senza alcun valore vincolante, ha tentato di individuare i principi regolatori di internet, *La dichiarazione dei diritti in Internet* in *https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf*. In dottrina su tale specifico documento G. De Minico, *Towards an Internet Bill of Rights*, in *Federalismi.it*, 2016; M.Bassini, O. Pollicino (a cura di), *Verso un Internet Bill of Rights*, Roma, 2015; A. Morelli, I *diritti e la Rete. Notazioni sulla bozza di Dichiarazione dei diritti in Internet*, in *Federalismi.it*, 1, 2015; S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014.

[30] Federal Communications Commission *Open Internet Order*, December 21, 2010, in *https://docs.fcc.gov/public/attachments/FCC-10-201A1.pdf*.

[31] R*egulation* (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 *laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services* 1-18. Per un primo e analitico commento sul Regolamento si v. M. Orofino, *La declinazione della net-neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un 'Internet aperta'*, in *Federalismi.it*, 21 novembre 2016, 1-25.

vamente ai c.d. servizi specializzati e alla possibilità di evitare la congestione di traffico, mentre nessuna esplicita menzione era fatta al divieto dello *zero rating*, la cui applicazione indiscriminata senza limiti chiari avrebbe potuto vanificare l'intento antidiscriminatorio della *regulation* unionale[32]. Non è possibile né è questa la sede per ripercorrere le varie fasi di applicazione del Regolamento, ciò che premere ricordare è che il *Body of European Regulators for Electronic Communications* (d'ora innanzi BEREC), secondo quanto previsto dall'Atto europeo, elaborò le prime linee guida nel 2016 per poi aggiornarle nel 2020 e nel 2022, in ragione della difficoltà di individuare in maniera sempre più specifica il punto di equilibrio fra applicazione del Net e la modalità di esercizio delle deroghe consentite. Come si diceva innanzi il Regolamento (UE) è stato progressivamente integrato dall'interpretazione della Corte di Giustizia, in particolare con le sentenze del 2 settembre 2021 (cause Telenor[33] *Vodafone e Deutsche Telekom*[34] e da ultimo *Telekom România Mobile Communications*[35] che hanno portato il BEREC a rivedere le proprie *guidelines* nel 2022, orientate ad sostanziale illiceità delle offerte di *zero-rating* in quei casi in cui la pratica favorisca alcune applicazioni al termine del *plafond* dati o combinino esenzioni commerciali con blocchi generalizzati del traffico concorrente.

---

[32] Sulla incompatibilità della partica dello *zero rating* con la net neutrality si vedano ancora G. De Minico, *op. cit.*, 27 e M. Avvisati, *Autorità Indipendenti, vigilanza e procedimento amministrativo. Il caso zero rating*, in *Politica del diritto*, 2/2017, 505-542.

[33] Corte di giustizia, 15 settembre 2020, cause riunite C-807/18 e C-39/19, *Telenor Magyarország Zrt. c. Nemzeti Média- és Hírközlési Hatóság Elnöke*, in *https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-09/cp200106en.pdf*. con commento di G. d'Ippolito, M. Monti, *Net neutrality e "tariffe zero": la convergenza delle esigenze democratiche e di mercato*, in *Medialaws*.

[34] Corte di Giustizia, C-854/19, 2 settembre 2021, *Vodafone GmbH, contro Bundesrepublik Deutschland*; C-5/20, 2 settembre 2021, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband contro Vodafone GmbH*, e C-34/20 *Telekom Deutschland GmbH contro Bundesrepublik Deutschland*.

[35] Corte di Giustizia, Sentenza n. C-367/24, 10 luglio 2025 *Autoritatea Națională pentru Administrare și Reglementare în Comunicații contro Telekom România Mobile Communications*, *Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband contro Vodafone GmbH*, e C-34/20 *Telekom Deutschland GmbH contro Bundesrepublik Deutschland.*

Il Regno Unito, dunque, si è conformato alle regole europee sino al 2023 anno in cui Ofcom ha introdotto una nuova *soft regulation*[36]. L'approccio utilizzato dal regolatore britannico è, rispetto al modello europeo (quest'ultimo non integralmente abbandonato) improntato ad una maggiore flessibilità nel senso che, fermo restando l'applicabilità, in via generale del principio, sono sia previste alcune modifiche in grado di assicurare sia lo sviluppo e innovazione della rete sia la tutela degli utenti. Secondo Ofcom, infatti, la presenza di alcuni elementi di rischio quali l'aumento esponenziale del traffico (streaming, cloud, gaming, realtà virtuale), la presenza dominante di pochi *content providers* che esercitano pressioni economiche sulle reti fisse e mobili e un eccessivo irrigidimento regolatorio potrebbero, combinati fra loro, limitare le altissime potenzialità innovative degli *Internet Service provider*s (d'ora innanzi ISPs). Per evitare che tali fattori frenino la concorrenza [37] l'Autorità di settore ha ritenuto di autorizzare a commercializzare pacchetti *specialised services* e *premium quality retail offers* (VR, gaming, servizi professionali)[38], in virtù del quali gli ISPs possono derogare al principio della neutralità della rete. È consentito anche un uso più ampio del *traffic management* se basato su esigenze tecniche oggettive purché proporzionato, temporaneo, non discriminatorio tra contenuti e non fondato su ragioni commerciali[39]. Infine, Ofcom ha aperto alla più discussa delle deroghe alla Net che è lo *zero-rating* in linea di principio ammissibile a condizione che non si detragga il consumo di dati di specifiche app dal *plafond* dell'utente mentre sono vietate quelle ipotesi di vietato zero-*rating* selettivo che hanno finalità palesemente anticompetitiva[40].

In altri termini, mentre nell'UE la neutralità tende a essere letta come divieto quasi assoluto di selezione commerciale tra flussi di traffico, nel contesto britannico essa è reinterpretata come divieto di

---

[36] Ofcom, *Net Neutrality Review*, 26 October 2023, in *https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/245902-net-neutrality-review/associated-documents/statement-net-neutrality-review?v=330310*.

[37] Ofcom, *Net Neutrality Review*, cit., 3; 125-145.

[38] Ofcom, *op. cit.*, 4, 9-102.

[39] Ofcom, *op. cit.*, 4, 67-91.

[40] Ofcom, *op. cit.*, 4, 39-67.

discriminazioni arbitrarie o opache, lasciando spazio a una certa "fantasia" commerciale considerata compatibile con l'*Open Internet*.

L'approccio dell'Autorità di regolazione britannica sembra ricalcare, dunque, l'impostazione adottata dalla Federal Communication Commissione statunitense (prima che *Restoring Internet Freedom Order* 2017[41]) con l'*Open Internet Order* 2015, precedentemente richiamato, che si orientava verso di un'analisi *case by case* ritenuta rispettosa del bilanciamento fra tutela dei diritti dell'utente e competizione.

Ofcom ha, di recente, affrontato anche la questione del *fair share* o *charging regime* (tema molto presente nel dibattito UE[42]) riguardante la possibilità che gli ISPs siano addebitati costi aggiuntivi ai *content providers* (es. Netflix, Google) per l'uso intensivo delle reti. Una misura che senza dubbio potrebbe apportare benefici in termini economici e di efficienza ma tali forme di regolazione non sono state considerate, al momento necessarie nel Regno Unito, anche perché un eventuale intervento spetta al decisore politico non essendo l'introduzione di tali misure di competenza dell'Autorità di settore. La neutralità della rete in UK, dunque, non è abbandonata, ma riconfigurata come principio compatibile con un Internet più complesso, caratterizzato da esigenze differenziate di qualità, bassa latenza e capacità di rete.

---

[41] Federal Commuinication Commition, *Restoring Internet Freedom, Declaratory Ruling, Report and Order*, 33 FCC Rcd 311 (2017) (Restoring Internet Freedom Order or Order) in *https://nsarchive.gwu.edu/document/20557-declaratory-ruling-report-and-order-and-order*.

[42] Nel 2023 la Commissione Europea ha avviato la consultazione dal titolo *The future of the electronic communications sector and its infrastructure*, disponibile *in www.digital-strategy.ec.europa.eu*, In favore di una condivisione degli investimenti commerciali M. Draghi, *The future of European competitiveness. Part. A., A competitiveness strategy for Europe*, 2024, 35, disponible in *www.commission.europa.eu*. Critico il BEREC, in BEREC *Preliminary assessment of the underlying assumptions of payments from large CAPs to ISPs*, 7 October 2022, in *https://www.berec.europa.eu/en/document-categories/berec/opinions/berec-preliminary-assessment-of-the-underlying-assumptions-of-payments-from-large-caps-to-isps?language_content_entity=en* che, invece, ha sottolineato i rischi di un simile regime in termini di sfruttamento del monopolio di terminazione, distorsioni nel mercato dell'interconnessione IP e necessità di una nuova ondata di regolazione *ex ante* del livello *wholesale*. In dottrina si v. G. Buttarelli, *La concorrenza tra stati e big tech nell'esercizio della sovranitá: il caso Meta*, in *IRPA Working Papers*,1/2025, in particolare 203, che aderisce all'impostazione di M. Draghi.

## 2. *La protezione dei dati personali nel Regno Unito post-Brexit*

### 2.1. *Dall'UK GDPR al (mancato) Data Protection and Digital Information Bill*

Con riguardo alla tutela del diritto fondamentale alla protezione dei dati personali, il Regno Unito ha adottato, nel periodo successivo alla Brexit, un approccio dinamico e, per molti aspetti, differenziato rispetto al modello europeo continentale. Il *Data Protection Act* 2018 (d'ora innanzi DPA)[43] ha rappresentato la prima fonte normativa di riferimento, dopo la separazione dalla UE anteriormente alla conclusione del periodo transitorio della Brexit. A seguito dell'*UK Trade and Cooperation Agreement* (d'ora innanzi TCA), stipulato nel dicembre 2020, ciascuna delle parti ha conservato un distinto e autonomo diritto di regolamentazione. La Gran Bretagna ha recepito una versione emendata del Regolamento (UE) 2016/679 (d'ora innanzi GDPR) nell'ordinamento interno, dando vita all'UK GDPR mediante modifiche al DPA. Va ricordato altresì che ai sensi del *European Withdrawl Act* del 2018 le normative sovranazionali incorporate nel diritto inglese mantenevano la primazia rispetto il diritto inglese. Nel 2023 con il *Reteined EU Law (revocation and reform) Act*[44] ha sancito il superamento della diretta applicabilità dei principi del diritto interno unionale alla legislazione domestica inclusi i diritti fondamentali derivanti dalla carta contenuta nel Trattato di Lisbona.

Ne è derivato un ampio margine di discrezionalità in materia di protezione dei dati, anche in considerazione del fatto che la Carta dei diritti fondamentali dell'Unione Europea non fa più parte del sistema giuridico dello Spazio Economico Europeo (SEE) e gli Stati membri del SEE non sono tenuti a aderirvi né a incorporarla nei rispettivi ordinamenti. Nel Regno Unito la tutela dei dati personali trova il suo principale fondamento nell'art. 8 CEDU, inteso prevalentemente come diritto alla vita privata. Ai sensi dello *Hu-*

[43] *Data Protection Act* 2018, in *https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted*.

[44] *Retained EU Law (Revocation and Reform) Act* 2023, in *https://www.legislation.gov.uk/ukpga/2023/28/contents*.

*man Rights Act* 1998[45], le Corti britanniche sono tenute a interpretare la legislazione in modo compatibile con i diritti sanciti dalla Convenzione «nella misura in cui ciò sia possibile», secondo un'ermeneutica generalmente meno espansiva rispetto a quella teleologica adottata dalla Corte di giustizia e dalla Corte Europea dei Diritti dell'Uomo[46].

Per quanto concerne i flussi di dati tra Regno Unito e Unione Europea, la tenuta del criterio di adeguatezza è risultata sin dall'inizio cruciale. Con decisione di esecuzione del 28 giugno 2021, la Commissione Europea ha riconosciuto il livello adeguato di protezione dei dati personali garantito dal Regno Unito ai sensi del GDPR[47]. I dati potevano quindi circolare liberamente dall'UE al Regno Unito, a condizione che quest'ultimo mantenga un livello di protezione sostanzialmente equivalente a quello europeo.

La Commissione ha valorizzato, tra l'altro, l'impianto particolarmente rigoroso di tutela della *privacy* nel settore dell'accesso ai dati da parte delle autorità pubbliche per finalità di sicurezza nazionale. La raccolta di dati da parte dei servizi di intelligence è subordinata, in linea di principio, a un'autorizzazione preventiva di un organo giurisdizionale indipendente; ogni misura deve risultare necessaria e proporzionata rispetto agli scopi perseguiti, e il soggetto interessato poteva adire *l'Investigatory Powers Tribunal* in caso di sospetta sorveglianza illegittima[48].La decisione di adeguatezza presentava tuttavia una significativa *sunset clause*, in virtù

---

[45] *Human Rights Act* 1998, *https://www.legislation.gov.uk/ukpga/1998/42/contents*.

[46] E. Celeste, *The Adequacy Decision for the UK: An Island of Data Protection in a Sea of Uncertainties*, in *Eur. Data Protection Law Rev*, vol. 7, n. 3, 2021; K. Mc Cullagh *Post-Brexit data protection in the UK - leaving the EU but not EU data protection law behind*, in G. González, R. Van Brakel, P. De Hert (a cura di), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, London, 2022.

[47] European Commission, Implementing *decision (EU) 2021/1773 of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, in *Official Journal of the European Union* L 360/69, 11.10.2021.

[48] K.Mc Cullagh, *The Investigatory Powers Tribunal: A UK Model for Rights Protection in Intelligence and Law Enforcement?*, in *European Public Law*, vol. 28, n. 2, 2022.

della quale essa avrebbe dovuto perdere efficacia dopo quattro anni, ossia il 27 giugno 2025. In realtà in data 19 luglio 2025 è intervenuta l'approvazione del *Data Use Access Act*[49], (d'ora innanzi DUAA) una nuova riforma che dovrebbe rappresentare un parziale superamento sia del UK GDPR sia delle normative intervenute dopo l'uscita del Regno Unito dall'Europa, che hanno imposto un ritardo nella valutazione di adeguatezza da parte dell'Unione Europea.

Già in precedenza era stato proposto un progetto di riforma radicale della disciplina, dai due Primi Ministri Conservatori, Boris Johnson e Rishi Sunaki i *Data Protection and Digital Information Bill* [50] che aveva suscitato diffusi timori circa un possibile deterioramento del livello di tutela dei diritti fondamentali.

Il disegno di legge mirava, tra l'altro, a introdurre maggiori margini di flessibilità nell'utilizzo dei *cookie*, ad ampliare l'uso di processi decisionali automatizzati e a sostituire i *Data Protection Officers* con «soggetti responsabili senior». Esso attribuiva inoltre al Governo poteri penetranti di intervento tramite l'*Information Commissioner*, rafforzando il regime sanzionatorio amministrativo. La clausola 5 chiariva che gli «interessi legittimi» potevano essere invocati come base giuridica per il *marketing* diretto, eliminando il test di bilanciamento in relazione a determinati interessi pubblici; la clausola 9 consentiva alle autorità pubbliche di respingere alcune richieste di accesso ai dati (Subject Access Requests); la clausola 14 introduceva una presunzione di legittimità delle decisioni automatizzate, riformulando l'art. 22 GDPR ed escludendo limitazioni incisive alla profilazione; la clausola 20, infine, ridisegnava le valutazioni d'impatto sui trattamenti ad alto rischio, attenuando gli obblighi informativi e di documentazione[51].

---

[49] *Data (Use and Access) Act* 2025, in *https://www.legislation.gov.uk/ukpga/2025/18/contents*.

[50] Il disegno di legge è stato presentato due volte e la seconda versione è stata leggermente modificata tant'è che vi sono un *Data Protection and Digital Information Bill* 1 e 2.

[51] Un'approfondita e dettagliata analisi delle criticità di questo disegno di legge è contenuta in F. Mazzi, A. Adonis, J. Cowls, A. Tsamados, M. Taddeo, L. Floridi *The UK reform of data protection: key changes, and their ethical, social and legal implication*; in *International Journal of Law and Information Technology*, 2022, 30, 269-279. E. Celeste, *Data Protection and Digital Sovereignty Post-Brexit: An Introduction*, in

Dottrina autorevole aveva segnalato come tali modifiche potessero mettere a rischio la decisione di adeguatezza con l'UE, in quanto il Regno Unito non avrebbe più garantito un livello di protezione «sostanzialmente equivalente» a quello europeo[52]. Il Bill non è stato tuttavia approvato a causa delle dimissioni del governo e le nuove elezioni ed è stato superato, dopo un iter parlamentare relativamente rapido, dall'adozione del *Data (Use and Access) Act* 2025, già richiamato.

### 2.2. *Il Data (Use and Access) Act 2025: semplificazione, innovazione e tenuta dell'adeguatezza*

Il *Data (Use and Access) Act* ha ottenuto il *Royal Assent* il 19 giugno 2025 dando attuazione alle linee di riforma prefigurate dalla consultazione *Data: a new direction* del 2021[53]. La normativa interviene nel quadro post-Brexit incidendo sull'UK GDPR, sul *DPA* 2018 e sulle *Privacy and Electronic Communications Regulations*, con l'obiettivo di coniugare semplificazione degli adempimenti, certezza giuridica e promozione dell'innovazione digitale.

Il DUAA consta di 144 sezioni e sedici allegati, dedicati a temi eterogenei quali sistemi di *smart data*, verifiche di identità digitale, creazione del *National Underground Asset Register* e digitalizzazione della registrazione di nascite e decessi e disposizioni in ordine ai trattamenti per finalità di *law enforcement* (Parte 3 DPA 2018) e quelli dei servizi di intelligence (Parte 4 DPA 2018).

L'entrata in vigore del DUAA è graduale: la maggior parte delle disposizioni richiede l'adozione di *Statutory Instruments*, con applicazione prevista intorno a dicembre 2025; alcune norme sono divenute efficaci automaticamente due mesi dopo il *Royal Assent*

---

E. Celeste, Róisín Á Costello, Edina Harbinja, Napoleon Xanthoulis (a cura di), *Data Protection and Digital Sovereignty Post-Brexit*, London, 2023.

[52] Per una ricostruzione più analitica del contenuto originario del *Data Protection and Digital Information Bill* e dei suoi profili critici ai fini dell'adeguatezza v. J. Tozer, *The Data Protection and Digital Information Bill: A Threat to UK Adequacy?*, in *J. Data Protection & Privacy*, vol. 7, n. 2, 2024; D. Erdos, *The UK's Proposed Data Protection Reforms: Implications for Adequacy and Rights*, in *Int. Data Privacy Law*, vol. 14, n. 1, 2024.

[53] *National Data Strategy*, in *https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy*.

(20 agosto 2025), altre già dal 19 giugno 2025. Tale stratificazione temporale impone ai soggetti interessati un monitoraggio costante della normativa secondaria per consentire alle imprese di potersi adeguare tempestivamente alle nuove norme.

Tra le innovazioni di maggior rilievo si segnala la ristrutturazione dei diritti degli interessati in materia di reclami. Il DUAA ha previsto un meccanismo a doppio per il livello per i reclami presentati dagli utenti. Questi, infatti saranno gestiti in prima battuta dai titolari del trattamento, imponendo l'adozione di strumenti agevoli (inclusi moduli elettronici), tempi di risposta definiti (30 giorni) e obblighi di trasparenza circa l'avanzamento e l'esito delle istanze e solo in un secondo momento i reclami potranno essere presentati all'Autorità di settore. Si tratta di una misura che dovrebbe non solo rendere più semplice e veloce la risposta ad eventuali violazioni ma anche alleggerire l'attività della riformata *Authority*.

Il *Digital Use and Access Act* muta in modo significativo la struttura di *governance* e *accountability* dell'*Information Commissioner's Office* (d'ora in poi ICO) che diviene *Information Commission* (d'ora innazi IC), un nuovo organismo statutario composto da membri esecutivi e non esecutivi e soggetto all'indirizzo strategico del *Secretary of State*, superando il precedente modello incentrato su un singolo Commissario. La riforma avvicina l'assetto istituzionale dell'IC a quello di altri regolatori economici del Regno Unito, quali la *Financial Conduct Authority* e la *Competition and Markets Authority*. Parallelamente, vengono ridefiniti i poteri dell'IC che è ora legittimato a richiedere relazioni, a esigere la produzione di documenti e a svolgere attività ispettive anche tramite convocazioni individuali.

La riforma attribuisce il *Secretary of State* il potere di emanare linee guida vincolanti sulle modalità di esercizio delle funzioni della *Commission*, anche in relazione alla definizione delle priorità dell'attività regolatoria. Tali orientamenti sono soggetti a consultazione pubblica, ma possono incidere sull'esercizio del potere discrezionale di *enforcement*[54].

[54] L'intera disciplina sulla riforma dell'ICO è contenuta nella Schedule 14, che emenda la Parte 5 and aggiunge una nuova Schedule 12A del DPA 2018 nonché riforma la Sezione 155 del DPA 2018.

Questo mutamento di governance si inserisce in un più ampio riallineamento del quadro britannico di protezione dei dati verso obiettivi di carattere economico e innovativo. Al contempo, solleva interrogativi circa la capacità della nuova Authority di agire quale autorità di controllo autonoma ai fini della cooperazione transfrontaliera. Il GDPR che richiede che le autorità di vigilanza esercitino le proprie funzioni in completa indipendenza senza ingerenze politiche. Il DUAA introduce, invece, un intervento da parte del *Secretary of State*, sollevando preoccupazioni in merito al rischio di condizionamento politico e sulla imparzialità dell'I*nformation Commission*. Pur permanendo garanzie quali il sindacato giurisdizionale e la consultazione pubblica, il possibile ridimensionamento dell'autonomia dell'IC potrebbe rendere più complessa la cooperazione con le autorità UE/SEE o futuri negoziati in tema di adeguatezza[55].

Particolare attenzione, nella riforma approvata, è dedicata ai trattamenti per finalità di ricerca, archiviazione e statistiche (*RAS Purposes*), il cui regime viene chiarito quanto ad ambito di applicazione, compatibilità con le finalità originarie, requisiti di consenso per la ricerca scientifica e garanzie tecniche quali la pseudonimizzazione e misure di sicurezza proporzionate[56].

La sezione 67 modifica l'art. 4 dello UK GDPR chiarendo che il trattamento di dati personali per finalità di ricerca scientifica comprende qualsiasi attività di ricerca che possa ragionevolmente essere qualificata come scientifica, indipendentemente dal fatto che

---

[55] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - ICO Reform*, 2.7.2025 in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-ico-reform/1-6*. Analoga criticità è stata rilevata in dall'European Data Procection Board, *Opinion 27/2025 regarding the European Commission Draft Implementing Decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data by the United Kingdom*, 16 October 2025, reperibile in *https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-272025-regarding-european-commission-draft_it*, 15.

[56] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Recognised Legitimate Interests (RLIS) The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Recognised Legitimate Interests (RLIS)*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-recognised-legitimate-interests-rlis/*.

sia finanziata pubblicamente o privatamente e dalla sua natura commerciale o non commerciale. In tale nozione rientrano lo sviluppo tecnologico, la ricerca fondamentale e applicata, nonché gli studi di sanità pubblica. La sezione 68 modifica l'art. 6(2) dello UK GDPR consentendo l'utilizzo del consenso ampio (*broad consent*) nei contesti di ricerca. Quando le finalità specifiche non possano essere definite in modo completo al momento della raccolta del consenso, quest'ultimo può comunque considerarsi valido se conforme agli standard etici generalmente riconosciuti nel settore della ricerca oppure sia possibile, prestare il consenso solo ad alcune parti del progetto di ricerca. Questa soluzione recepisce l'approccio del considerandum 33 del GDPR, ma lo trasforma in norma vincolante nel diritto britannico. Il trattamento per finalità di ricerca è ammesso soltanto per la raccolta di dati personali (presso l'interessato o da altre fonti) e se i dati vengono trasformati in informazioni non identificabili e che la finalità RAS non può essere ragionevolmente raggiunta senza tale trattamento. I titolari devono adottare garanzie per i diritti e le libertà degli interessati, tra cui la pseudonimizzazione e la separazione funzionale rispetto ad altre finalità. Il *Secretary of State* può specificare tramite regolamento quali garanzie costituiscono misure appropriate ai sensi dell'art. 84B (2), ma non può modificare le garanzie sostanziali previste dai paragrafi 2-4 dell'art. 84C.

La modifica ha importanti implicazioni per università, enti di ricerca ma anche imprese private in quanto positivizza quanto era solo suggerito dal considerando 50 del GDPR, creando un regime basato su regole certe giuridica e riduce la necessità di richiedere nuovamente il consenso o di individuare nuove basi giuridiche per il riuso dei dati, qualora gli obblighi legislativi siano soddisfatti. Il limite di questa disposizione è l'ampiezza della definizione ricerca scientifica. Com'è stato opportunamente osservato la norma non chiarisce se i soggetti richiedenti sono istituti di ricerca finanziati con soldi pubblici o privati e se il fine della ricerca è commerciale o non commerciale esponendo al rischio di un'illegittima e non sempre chiara utilizzazione a scopi economici i dati stessi molti dei quali, presumibilmente, rientranti nella categoria di dai sensibili. Del resto, le garanzie di pseudonimizzazione, minimizzazione dei

dati e separazione funzionale rispetto ad altre finalità, com'è noto non sempre garantiscono la non identificabilità del soggetto i cui *data set* si riferiscono[57].

Quanto alle decisioni automatizzate il DUAA introduce alcune importanti aggiornamenti attenuando le più stringenti previsioni rispetto alla normativa precedente.

Il DUAA, infatti, abroga e sostituisce integralmente il previgente regime dell'art. 22 GDPR, introducendo un nuovo *corpus* normativo (artt. 22A-22D UK GDPR) dedicato alla disciplina delle *Automated Decision Making* (d'ora innanzi ADM). La riforma riscrive le soglie applicative, le garanzie e i poteri pubblici in materia delle ADM collocando tali elementi entro una cornice legislativa più dettagliata di quanto non facesse il GDPR. L'art. 22A introduce la nozione di *significant decision*, intesa come decisione idonea a produrre effetti giuridici o, comunque, con conseguenze di analoga rilevanza per l'interessato. Una decisione è considerata «basata unicamente su un trattamento automatizzato» quando difetti di un coinvolgimento umano significativo; la nozione di *meaningful human involvement* non è puntualmente definita dal legislatore, ma l'art. 22D attribuisce al *Secretary of State* il potere di precisarne la portata mediante regolamenti. L'art. 22B pone un divieto rafforzato: è preclusa l'adozione di *significant decisions* fondate esclusivamente su dati sensibili, salvo che l'interessato abbia prestato un consenso esplicito oppure che la decisione sia richiesta o autorizzata dalla legge e ricorrano le condizioni dell'art. 9(2)(g) UK GDPR. La riforma introduce così un test autonomo nel diritto britannico, ampliando l'ambito applicativo alle decisioni in cui i dati sensibili costituiscano solo una parte del trattamento. L'art. 22C tipizza le garanzie minime applicabili a ogni decisione significativa adottata tramite processi automatizzati. Il titolare è, infatti, tenuto a: informare l'interessato dell'esistenza di un processo decisionale automatizzato; consentirgli di presentare osservazioni; riconoscere il diritto a un intervento umano, su richiesta o quando previsto dalla legge;

[57] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Scientific, historical and statistical purposes*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-scientific-historical-and-statistical-purposes/*, 1-7.

permettere la contestazione della decisione. L'art. 22D (3) autorizza, inoltre, il *Secretary of State* a integrare (ma non a ridurre) la definizione di decisione automatizzata e il catalogo delle garanzie, mediante regolamenti adottati in via secondaria[58].

Il nuovo regime riproduce in parte la struttura del modello europeo, ma ne modifica la tecnica normativa. Le garanzie, già previste dall'art. 22 GDPR e dai relativi considerando, assumono ora la forma di obblighi espressamente codificati dal legislatore britannico. Il risultato è duplice: da un lato, una maggiore chiarezza definitoria in particolare quanto alle soglie di applicazione e alla copertura delle decisioni parzialmente automatizzate che utilizzano dati sensibili; dall'altro, un'espansione del potere regolamentare del *Secretary of State*[59].

Il DUAA estende il regime generale relativo alle ADM introdotto dagli artt. 22A-22D dello UK GDPR, anche alla Parte 3 (trattamenti per finalità di *law enforcement*) e alla Parte 4 (trattamenti da parte dei servizi d'intelligence) del DPA 2018, assicurando così una coerenza sistemica tra disciplina generale e discipline settoriali in materia di protezione dei dati. Le nuove Sezioni 50A-50D introducono definizioni normative aggiornate di s*olely automated processing* e di *significant decision*. Queste ultime sono quelle che producono un effetto giuridico avverso o, comunque, effetti avversi di analoga rilevanza sull'interessato. Si tratta di una nozione più ristretta rispetto al regime generale, poiché tende a escludere dall'ambito di tutela gli esiti automatizzati non pregiudizievoli o neutri. Inoltre viene mantenuta una definizione di *solely automated* coerente con quella prevista dal regime generale dell'UK GDPR, includendo ora un obbligo esplicito di valutare il grado di profilazione coinvolto, positivizzando un elemento che, in precedenza, era frutto di elaborazione giurisprudenziale e di prassi regolatoria; vi è poi divieto di ADM basate su dati appartenenti a categorie partico-

[58] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Automated Decision-Making (ADM)*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-automated-decision-making-adm/*, 1-6.

[59] Esprime perplessità sulla nuova disciplina l'European Data Protection Board, cit., 9.

lari, salvo che ricorra una base giuridica specifica (ad es. una norma statale) o l'esplicito consenso dell'interessato, in conformità alla sezione 50B(4). Infine le diposizioni relative a questa parte consentono l'adozione di *significant decisions* basate unicamente su trattamenti automatizzati solo quando ciò sia richiesto o autorizzato dalla legge e a condizione che tale legge preveda adeguate garanzie. Tali garanzie devono includere almeno: il diritto all'intervento umano; il diritto di presentare osservazioni; il diritto di contestare la decisione. In ogni caso viene predisposta un'esenzione qualificata nel senso che qualora la normativa applicabile non contiene le già menzionate garanzie, il titolare può comunque ricorrere all'ADM purché "rivaluti la decisione non appena ragionevolmente possibile, mediante un intervento umano significativo. In tale ipotesi viene introdotta una garanzia *ex post* che non trova corrispondenza nel GDPR.

Le modifiche alla Parte 4 (Section 95-96) rispecchiano una r*egulation* analoga al regime generale, ma vi sono anche regole più specifiche. Viene definito l'*entirely automated decision-making* con riferimento ai trattamenti dei servizi di intelligence. Si tratta di una decisione adottata esclusivamente tramite mezzi automatizzati, senza che alcuna persona abbia esaminato, influenzato o autorizzato l'esito prima che esso produca effetti nei confronti dell'interessato. Anche in questo caso si stabilisce che una decisione non possa fondarsi esclusivamente su processi automatizzati, salvo che ciò sia autorizzato dalla legge, incluse regole interne previste dal quadro normativo dei servizi di intelligence Sono previste comunque, adeguate garanzie, come il diritto di contestare la decisione ma anche ampie deroghe nei casi in cui l'applicazione di tali garanzie possa compromettere la sicurezza nazionale, la sicurezza pubblica o la prevenzione o repressione dei reati.

Il modello britannico, che valorizza la revisione successiva alla decisione, si discosta sensibilmente dall'impostazione europea incentrata sul controllo umano preventivo, cioè prima che la decisione produca effetti. Sebbene il nuovo quadro normativo del Regno Unito, sia nella Parte 3 sia nella Parte 4, assicuri maggiore chiarezza legislativa, amplia la discrezionalità operativa in alcuni ambiti sensibili e soprattutto nella disciplina dei servizi di intelligence am-

mette la *post-facto reconsideration* quale meccanismo residuale di tutela, offrendo sì una maggiore flessibilità operativa alle agenzie competenti, ma una significativa compressione dei diritti fondamentali poché il soggetto destinatario vedrà applicarsi prima il provvedimento e poi successivamente e solo eventualmente una revisione grazie all'intervento umano[60].

Un'altra direttrice di intervento è la codificazione dei *Recognized Legitimate Interests* (d'ora innanzi RLI) come basi giuridiche esentate dal bilanciamento con i diritti e le libertà degli interessati in ipotesi specifiche, contenute in un elenco chiuso e che ricomprende: sicurezza nazionale, tutela di soggetti vulnerabili, emergenze, prevenzione e repressione dei reati. Quando un titolare comunica dati personali a un altro soggetto che li tratterà per uno degli RLI elencati, il titolare comunicante è esonerato dal compiere una *Legitimate Interests Assessment* (d'ora innanzi LIA), inclusa la consueta verifica di bilanciamento rispetto ai diritti e alle libertà dell'interessato. Rimane tuttavia applicabile il requisito di necessità, e la comunicazione deve essere strettamente indispensabile per la finalità specificata.

Il Segretario di Stato può modificare l'elenco degli RLI tramite normativa secondaria, tenendo conto dei diritti e delle libertà fondamentali degli interessati e della particolare protezione dovuta ai dati dei minori. Sebbene la riforma offra una certa flessibilità e capacità di intervento immediato nel fronteggiare nuovi rischi di interesse pubblico, introduce margini di incertezza giuridica per la limitata possibilità del Parlamento di incidere sull'approvazione di tale normativa, sollevando interrogativi in relazione al principio di legalità e alla prevedibilità della norma[61]. Il DUAA, poi, si discosta

[60] Sul punto si vedano in particolare i rilievi mossi dall'EUROPENA DATA PROCECTION BOARD, *op. cit.*, in particolare 9. N. MORENO, C. MELTON, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - ADM in Law Enforcement and National Security*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-adm-in-law-enforcement-and-national-security/*, 1-7.

[61] N. MORENO, C. MELTON, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Recognised Legitimate Interests (RLIS)*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-recognised-legitimate-interests-rlis/*, 1-6.

dall'approccio caso-per-caso e sensibile al contesto previsto dal GDPR, che si fonda sull'obbligo di condurre una LIA completa.

La riforma modifica il principio della limitazione della finalità di cui all'articolo del UK GDPR riscrivendo il quadro di compatibilità previsto che disciplina i trattamenti ulteriori di dati personali. La modifica legislativa introduce condizioni di compatibilità e un nuovo articolo (8A) nel UK GDPR, supportato dai criteri riportati nell'Allegato 2. Tali disposizioni riducono la necessità di una valutazione tradizionale della compatibilità quando ricorrono specifiche condizioni giuridiche e di policy. Nel sistema del GDPR, i titolari devono valutare se la finalità ulteriore sia compatibile con quella originaria di raccolta, utilizzando i criteri contestuali quali il legame con la finalità iniziale, il contesto della raccolta, la natura dei dati e le legittime aspettative dell'interessato.

La nuova legge sostituisce tale impianto con un modello differente per il trattamento ulteriore, individuando le circostanze in cui la valutazione di compatibilità *ex* articolo 6(4) UK GDPR non è richiesta o risulta semplificata. Tali differenti modalità di valutazione del trattamento ulteriore sono codificate nel nuovo articolo 8A, che introduce una disciplina nella quale vengono elencati gli scenari di trattamento ulteriore esentati dalla valutazione. L'articolo 8A (3) rinvia poi all'Allegato 2, che elenca specifiche ipotesi di trattamenti considerati compatibili senza necessità di un'ulteriore valutazione: se l'interessato presta il consenso al trattamento ulteriore e la nuova finalità è specifica, esplicita e legittima; se il trattamento ulteriore sia effettuato per ricerca scientifica o ricerca storica, archiviazione nel pubblico interesse o finalità statistiche. Sono comunque previste garanzie es. minimizzazione, pseudonimizzazione). Infine, il trattamento ulteriore non richiede consenso se la comunicazione dati personali avviene in risposta alla richiesta di un altro soggetto che li necessita per svolgere un trattamento per finalità di pubblico interesse o esercizio di pubblici poteri sulla base di una previsione normativa e il trattamento è necessario per tutelare sicurezza pubblica, tutela dell'indipendenza giudiziaria o esecuzione di pretese civili. Il titolare comunicante non deve essere un'autorità pubblica che svolge i propri compiti istituzionali. In tutti i casi, il trattamento ulteriore deve comunque rispettare i principi di correttezza e traspa-

renza di cui all'articolo 5 e, se del caso, devono essere applicate garanzie adeguate, in particolare quelle previste dall'articolo 89(1). Il Segretario di Stato può ampliare o modificare tale elenco mediante regolamento. Tale meccanismo introduce flessibilità, ma ancora una volta solleva anche dubbi relativi al principio di legalità, alla prevedibilità e all'ampiezza della discrezionalità ministeriale.

La riforma crea dunque un modello a due livelli del trattamento ulteriore nel Regno Unito.

Tuttavia, la valutazione su quali dati fornire in quanto compatibili va fatto dal titolare del trattamento che non sempre è in grado di effettuare il test di proporzionalità e necessità soprattutto quando il trasferimento viene effettuato ai fini di sicurezza nazionale o per i casi in cui la deroga è consentita. Il timore espresso nei primi commenti alla legge è che tale meccanismo possa essere utilizzato dalle autorità pubbliche per aggirare i limiti legali alla raccolta di dati o ottenere più dati rispetto a quelli strettamente necessario ovvero l'utilizzo improprio dei dati per l'addestramento dell'AI generativa[62].

Sul versante dei trasferimenti internazionali di dati, il DUAA recepisce un approccio *risk-based*, nel senso che il trasferimento può essere autorizzato se gli standard non sono inferiori alla regolazione vigente in UK e attribuendo al *Secretary of State* poteri ampliati di monitoraggio e intervento sulle decisioni di trasferimento. Si tratta di un criterio più blando rispetto a quello del criterio di adeguatezza, contenuto tra l'altro, nel precedente UK GDPR Act e DPA. La previsione più morbida espone a una serie di vulnerabilità del *data transfer* da UK verso paesi terzi, come ad esempio Stati Uniti e Cina, che notoriamente hanno un approccio meno garantisca alla tutela dei dati[63].

---

[62] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Purpose limitation*, *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-purpose-limitation/*, 1-6.

[63] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - International data transfers*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-international-data-transfers/*, 1-7.

Per quanto concerne i *cookies* e gli strumenti di tracciamento, la riforma introduce modifiche rilevanti al *Privacy and Electronic Communications Regulations* 2003 (d'ora innanzi PECR), ampliando l'elenco delle tipologie di *cookies* che possono beneficiare dell'esenzione dall'obbligo di consenso preventivo previsto dal PECR. Oltre ai *cookies* strettamente necessari, il consenso non è più richiesto quando tecnologie analoghe rientrano nelle nuove categorie di trattamenti a basso rischio, purché siano strettamente necessari per una delle finalità esentate (ad es.finalità statistiche/analitiche volte al miglioramento del servizio; sicurezza dei sistemi o rilevazione delle frodi; miglioramento della funzionalità del servizio o personalizzazione dell'interfaccia utente; aggiornamenti software o ottimizzazione dell'esperienza dell'utente; rilevazione di guasti o errori tecnici del servizio). I titolari devono comunque valutare se l'uso dei *cookies* sia strettamente necessario e se l'impatto sulla *privacy* richieda comunque il consenso dell'utente secondo un test di proporzionalità. Queste nuove esenzioni riflettono un passaggio a un approccio basato sul rischio, volto a ridurre richieste di consenso non necessarie (che generano *cookie fatigue*), pur mantenendo livelli di tutela elevati nei casi di rischio più significativo[64].

Viene estesa la regola del *soft opt-in*, prima riservata alle organizzazioni commerciali, anche ai soggetti non profit, quali enti di beneficenza, partiti politici e associazioni. Questi enti possono ora inviare comunicazioni di *direct marketing* tramite e-mail o SMS senza previo *opt-in*, a condizione che i dati di contatto siano stati raccolti nel corso di una precedente interazione; il *marketing* riguardi attività o finalità analoghe; sia fornita all'interessato una chiara possibilità di *opt-out* al momento della raccolta dei dati e in ogni successiva comunicazione.

Infine, l'*Act* allinea i poteri sanzionatori dell'IC in materia di PECR al regime sanzionatorio dello UK GDPR. La sezione 155 del DPA 2018, come modificata, consente all'IC di irrogare sanzioni

[64] N. Moreno, C. Melton, *The UK DUA Act's Reform Pillars: Divergence from the EU GDPR - Cookies and PECR Reform*, in *https://www.kennedyslaw.com/en/thought-leadership/article/2025/the-uk-dua-act-s-reform-pillars-divergence-from-the-eu-gdpr-cookies-and-pecr-reform/*, 1-7.

amministrative in caso di violazione superando così il vecchio limite massimo di 500.000 sterline, che risultava inadeguato per imprese di grandi dimensioni e privo di reale effetto deterrente[65].

L'*Act* si caratterizza per gli ampi e discrezionali poteri del *Secretary of State* di derogare alla disciplina del DUUA, in linea generale e in particolare rispetto ai trasferimenti internazionali, le decisioni automatiche e la governance dell'IC, attraverso l'utilizzo di *Statutory Instrument*, quindi la regolazione secondaria che richiede un minor controllo da parte del Parlamento. In tal modo il legislatore inglese sembrebbe voler favorire lo sviluppo dell'Intelligenza Artificiale soprattutto quelle di nuova generazione attraverso un uso più libero dei *data set*, così da creare un mercato alternativo più competitivo ma autonomo rispetto sia ai colossi statunitensi e cinesi sia al mercato europeo. Una scelta che però non tiene conto dei possibili rischi associati ad un affievolimento della tutela dei diritti.

La Commissione ha completato il riesame del DUAA e ha avviato la procedura per una nuova decisione di adeguatezza, ritenendo che le modifiche legislative mantengano un livello di protezione sostanzialmente equivalente a quello dell'Unione. La nuova decisione nell'ipotesi di esito positivo, avrà durata semestrale rinnovabile, è soggetta a monitoraggio continuo e a revisioni almeno quadriennali, in considerazione anche della proposta di riforma del GDPR con l'introduzione dell'*Omnibus Regulation Digital Act* e dunque la necessità di verificare nuovamente la compatibilità delle modifiche introdotte in UK rispetto alla nuova regolazione unionale.

## 3. *Sovranità digitale e convergenza regolatoria tra telecomunicazioni e protezione dei dati*

L'analisi svolta consente di cogliere un *fil rouge* che attraversa la disciplina delle telecomunicazioni e quella della protezione dei dati personali nel Regno Unito post-Brexit: la ricerca di un equilibrio fra esigenze di sovranità regolatoria, promozione dell'innova-

[65] In base al DUUA le sanzioni applicabili sono così determinate: fino a 17,5 milioni di sterline o al 4% del fatturato annuo globale per le violazioni più gravi; fino a 8,7 milioni di sterline o al 2% del fatturato globale per violazioni meno gravi.

zione e mantenimento di un livello di integrazione sufficiente con il mercato unico europeo.

Nel settore delle telecomunicazioni, la strategia regolatoria dell'Ofcom punta a creare un ambiente favorevole agli ingenti investimenti in reti a banda ultralarga e tecnologie satellitari, senza rinunciare ai tradizionali strumenti di controllo del significativo potere di mercato dell'*incumbent* BT. La scelta di preservare una regolazione geografica differenziata e di spostare progressivamente la pressione regolatoria dai servizi legacy in rame ai servizi in fibra e ai prodotti ad alta capacità riflette la volontà di accompagnare la transizione tecnologica senza produrre eccessive trasformazioni regolatori.

Sul terreno della protezione dei dati, il passaggio dall'UK GDPR al DUAA segnala l'intento di costruire un modello sì autonomo, orientato alla semplificazione e alla flessibilità, ma al tempo stesso in grado di preservare la decisione di adeguatezza. La rinuncia al più radicale *Data Protection and Digital Information Bill* e l'adozione di un atto più equilibrato come il DUAA testimoniano la consapevolezza del valore economico e sistemico del libero flusso dei dati tra Regno Unito e Unione Europea. L'allineamento sostanziale alle garanzie del GDPR appare, almeno per il momento, la condizione necessaria per evitare una frammentazione eccessiva degli spazi di circolazione dei dati e per assicurare un'interoperabilità regolatoria minima con l'UE, fermo restando che la nuova disciplina non ignora la necessità di semplificare la *regulation* per non perdere l'opportunità di aprire ad altri mercati lo scambio di dati.

La strategia regolatoria dell'Ofcom e l'approvazione del DUUA rappresentano, dunque il primo esperimento in cui il Regno Unito tenta di raggiungere un complesso punto di equilibrio tra competizione, innovazione e garanzia dei diritti fondamentali. Un ordinamento quello britannico che non guarda più solo al mercato interno europeo ma alla dimensione effettivamente globale che le tlc hanno assunto in anni recenti.

In questo quadro la questione della sovranità digitale del Regno Unito si gioca su un crinale sottile talvolta ambiguo e contraddittorio motivato anche da ragioni di carattere geopolitico e finanziario. La crescente dipendenza da grandi operatori extraeuropei, principalmente nel settore satellitare e le politiche aggressive della

nuova Presidenza Trump e degli *Over the top* che rendono il Regno Unito una sorta di terra promessa nel cuore del vecchio continente, in grado di favorire un'espansione senza precedenti dei propri *data center* per lo sviluppo massiccio dell'Intelligenza Artificiale, applicate alla Sanità, e alla capacità del calcolo quantistico. Al di là del grande vantaggio economico che UK dovrebbe ottenere vi è la sensazione che il Regno Unito «si possa trasformare in un avamposto strategico e in uno strumento per frenare le ambizioni di autonomia tecnologica dell'Unione Europea[66]».

La Brexit non è dunque stata il passaggio da una sovranità politica limitata a una piena sovranità ma la transizione verso una sovranità limitata dal potere tecnologico ben più insidioso e pericoloso.

[66] V. Barretta, *Accordo USA-UK, la sovranità che non c'è*, in *Key4 Bitz*, 19 settembre 2025.

# NOTIZIE SUGLI AUTORI


Giovanna De Minico
*Professoressa ordinaria di Diritto costituzionale e pubblico presso l'Università degli Studi di Napoli "Federico II"*

Marco Orofino
*Professore ordinario di Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

Fulvia Abbondante
*Professoressa associata di Diritto costituzionale e pubblico presso l'Università degli Studi di Napoli "Federico II"*

Allegra Canepa
*Professoressa associata di Diritto dell'economia presso l'Università degli Studi di Milano*

Lavinia Del Corona
*Assegnista di ricerca in Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

Maria Francesca De Tullio
*Ricercatrice di Diritto costituzionale e pubblico (RTD-A) presso l'Università degli Studi di Napoli "Federico II"*

Antonio Foti
*Dottorando di ricerca in Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

Chiara Galbersanini
*Assegnista di ricerca in Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

Federico Gustavo Pizzetti
*Professore ordinario di Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

ANDREA RUFFO

*Assegnista di ricerca in Diritto costituzionale e pubblico presso l'Università degli Studi di Milano*

STEFANIA SERAFINI

*Professoressa associata di Diritto commerciale presso l'Università degli Studi di Napoli "Federico II"*

Finito di stampare
nel dicembre 2025
Print Sprint - Napoli