FASCICOLO SPECIALE

S. D'ACUNTO, B. NASCIMBENE, V. BACHELET, M. OROFINO, G. ZICCARDI, F. FERRI, P. KOWALICKA, M. CARTA, M. GUIDI, F. ROSSI DAL POZZO

IL MERCATO UNICO DIGITALE TRA ANTICHI PROBLEMI E NUOVE SFIDE

a cura di F. ROSSI DAL POZZO e I. ANRÒ

Il Mercato Unico Digitale
tra antichi problemi e nuove sfide
Fascicolo speciale
a cura di F. ROSSI DAL POZZO e I. ANRÒ

ISSN 2384-9169
Fascicolo speciale
Pubblicato nel mese dicembre del 2025, http://rivista.eurojus.it

Editore: Bruno Nascimbene, Milano
Rivista registrata presso il Tribunale di Milano, n. 278
del 9 settembre 2014
Eurojus © è un marchio registrato

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Co-funded by
the European Union

EU
intelligent internal
market

Summer School | PROGRAMMA

5 GIUGNO 2025

Università degli studi di Milano, via Santa Sofia, aula M401

Ore 9:00

Saluti istituzionali
Avv. Antonino La Lumia
Presidente del Consiglio dell'Ordine degli Avvocati di Milano
Avv. Cristiano Bacchini
Coordinatore della Commissione IP e Antitrust dell'Ordine degli Avvocati di Milano

Introduce e presiede:
Prof.ssa Ilaria Anrò,
Associato di diritto dell'UE, Università degli Studi di Milano, Jean Monnet Module Leader

Dott. Salvatore D'Acunto,
Capo Unità, DG Mercato Interno, Commissione europea
Il mercato unico dell'Unione europea: origini, strumenti e sviluppo.

Ore 11:00

Prof. Bruno Nascimbene,
Emerito di diritto dell'UE, Università degli Studi di Milano
Il mercato unico digitale quale nuova frontiera dell'integrazione europea.

Ore 12:30 LUNCH BREAK

Ore 14:30

Prof. Vittorio Bachelet,
Associato di Diritto Privato, Università Cattolica del Sacro Cuore, Milano
La tutela dell'impresa nel mercato unico digitale.

Ore 16:30

Avv. Giacomo Dalla Valentina,
Gianni&Origoni
Gatekeepers e nuove regole: alcuni casi pratici.

Ore 18:00 FINE DEI LAVORI

12 GIUGNO 2025

Università degli studi di Milano, via Santa Sofia, aula M402

Ore 9:00

Introduce e presiede:
Prof.ssa Ilaria Anrò,
Associato di diritto dell'UE, Università degli Studi di Milano, Jean Monnet Module Leader

Prof. Marco Bassini,
Assistant Professor of Fundamental Rights and Artificial Intelligence, Tilburg University
La responsabilità degli internet services providers, tra regole vecchie e nuove.

Ore 11:00

Prof. Francesco Rossi Dal Pozzo,
Ordinario di diritto dell'UE, Università degli Studi di Milano

Dott. Marco Guidi,
Ricercatore di diritto dell'UE, Università degli Studi di Roma Unitelma Sapienza
Il Digital Markets Act, un nuovo paradigma?

Ore 12:30 LUNCH BREAK

Ore 14:30

Prof.ssa Silvia Zorzetto,
Associato di Filosofia del diritto, Università degli Studi di Milano
Responsabilità civile e sistemi di intelligenza artificiale.

Ore 16:30

Prof.ssa Maria Lillà Montagnani
Ordinario di Diritto Commerciale, Università Bocconi, Milano
La governance dei dati nel digital single market.

Ore 18:00 FINE DEI LAVORI

19 GIUGNO 2025

Università degli studi di Milano, via Santa Sofia, aula M402

Ore 9:00

Introduce e presiede:
Prof.ssa Ilaria Anrò,
Associato di diritto dell'UE, Università degli Studi di Milano, Jean Monnet Module Leader

Prof.ssa Marilisa D'Amico,
Ordinario di diritto costituzionale, Università degli Studi di Milano

Prof. Francisco Balaguer Callejón,
Ordinario di diritto costituzionale, Università di Granada
La tutela dei diritti fondamentali e le nuove tecnologie.

Ore 11:00

Prof. Giovanni Ziccardi,
Ordinario di informatica giuridica, Università degli Studi di Milano
Fake news e disinformazione: tra i pericoli e le opportunità del web.

Ore 12:30 LUNCH BREAK

Ore 14:30

Prof. Mario Carta,
Ordinario di diritto dell'UE, Università degli Studi di Roma Unitelma Sapienza
Il Regolamento sull'intelligenza artificiale: una nuova regolamentazione per il futuro del mercato unico digitale.

Ore 16:30

Dott. Federico Ferri,
Ricercatore di diritto dell'UE, Università di Bologna
Il bilanciamento dei diritti fondamentali nel mercato unico digitale.

Ore 18:00 FINE DEI LAVORI

26 GIUGNO 2025

Università degli studi di Milano, via Santa Sofia, aula M402

Ore 9:00

Introduce e presiede:
Prof.ssa Ilaria Anrò,
Associato di diritto dell'UE, Università degli Studi di Milano, Jean Monnet Module Leader

D.ssa Giulia Agrati,
Assegnista di diritto dell'UE, Università degli Studi di Milano
Il Digital Services Act: una nuova cooperazione tra Commissione, autorità nazionali ed europee.

Ore 11:00

Prof. Marco Orofino,
Ordinario di diritto costituzionale, Università degli Studi di Milano
Il nuovo equilibrio tra circolazione e tutela dei dati nel mercato unico digitale.

Ore 12:30 LUNCH BREAK

Ore 14:30

Avv. Valeria Specchio,
Rosell
Tutela dei dati e piattaforme digitali.

Ore 16:30

Avv. Paolo Franco,
HwP
La tutela dei dati in ambito sanitario: tra regole europee e nazionali.

Ore 18:00 FINE DEI LAVORI

3 LUGLIO 2025

Università degli studi di Milano, via Santa Sofia, aula M402

Ore 9:00

Introduce e presiede:
Prof.ssa Ilaria Anrò,
Associato di diritto dell'UE, Università degli Studi di Milano, Jean Monnet Module Leader

Prof. Oreste Pollicino,
Ordinario di diritto costituzionale, Università Bocconi, Milano
Il Regolamento sull'Intelligenza Artificiale tra sfide e opportunità.

Ore 11:00

Dott.ssa Camilla Burelli,
Ricercatore di diritto dell'UE, Università degli Studi di Milano
L'attuazione del Regolamento IA in Italia.

Ore 12:00

D.ssa Paulina Kowalicka
Assegnista di ricerca in Informatica Giuridica, Università degli Studi di Milano
La regolamentazione dell'IA fuori dai confini europei.

Ore 12:30 LUNCH BREAK

Ore 14:30

Prof. Filippo Croci,
Ricercatore di diritto dell'UE, Università degli Studi di Milano
Digital Markets Act: Public e private enforcement.

Ore 16:30

Prof. Massimo Condinanzi,
Giudice della Corte di giustizia dell'UE, Lussemburgo

Prof.ssa Chiara Amalfitano,
Ordinario di diritto dell'Unione europea, Università degli Studi di Milano
Il mercato unico digitale nella giurisprudenza della Corte di giustizia dell'Unione europea.

Ore 18:00 FINE DEI LAVORI

8 LUGLIO 2025

Visita alla
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

Si ricorda che, nella domanda di iscrizioneoccorre specificare se si intende partecipare anche alla visita.

La Summer School è organizzata nell'ambito del modulo Jean Monnet dal titolo: EU inte(lligent) rnal market between new challenges and old obstcles –Finanziamento della Commissione europea: Call for Proposals 2024 ERASMUS-JMO-2024-HEI-TCH-RSCH, Proposal number: 101176197

INDICE

Premessa
di FRANCESCO ROSSI DAL POZZO e ILARIA ANRÒ……..……p. I

Il Mercato unico dell'Unione europea: origini, strumenti e sviluppo
di SALVATORE D'ACUNTO…….…….……..……...p. 1

Il Mercato Unico Digitale è una nuova frontiera dell'integrazione europea?
di BRUNO NASCIMBENE…..…….p. 11

La tutela dell'impresa nel Mercato Unico Digitale
di VITTORIO BACHELET ……..…….....p. 26

The new balance between data circulation and data protection in the Digital Single Market
di MARCO OROFINO..…….…….....……..…..p. 45

Il deepfake*: aspetti tecnici, regolamentazione, guerra ibrida ed equilibri geopolitici*
di GIOVANNI ZICCARDI..……..…….….p. 56

Profili evolutivi della dimensione esterna del Mercato Unico Digitale
di FEDERICO FERRI…….…….……...……...p. 71

Sovranità digitale e governance *globale: i profili giuridici delle politiche digitali nel mondo*
di PAULINA KOWALICKA….……...……..……..p. 107

*L'*AI Act *e il* risk-based approach *nel settore digitale dell'UE al crocevia tra elementi di continuità e innovazione*
di MARIO CARTA e MARCO GUIDI……..……...…..….p. 130

Il Digital Market Act*, un nuovo paradigma per la politica di concorrenza dell'UE nei mercati digitali: tra regolamentazione e diritto antitrust*
di FRANCESCO ROSSI DAL POZZO e MARCO GUIDI..…….……..p. 167

Premessa

Gli scritti raccolti in questo numero speciale nascono dalle relazioni che sono state tenute nell'ambito della *Summer School* "Il Mercato Unico Digitale tra antichi problemi e nuove sfide: una guida agli strumenti fondamentali di diritto dell'Unione europea", svoltasi a Milano tra il 5 giugno e il 3 luglio 2025. La *Summer School,* organizzata nell'ambito del modulo Jean Monnet dal titolo "EU inte(lligent)rnal market between new challenges and old obstacles"[1] è stata l'occasione per riunire accademici, funzionari delle istituzioni europee, avvocati, professionisti e studenti interessati ad approfondire i temi legati alle sfide poste dalle nuove tecnologie nell'ambito del mercato interno.

Come noto, fin dalle origini, il Mercato Unico Digitale mira a rimuovere le barriere nazionali alle transazioni *online* e a creare un ambiente sicuro in cui i diritti fondamentali e i valori dell'Unione europea siano tutelati, promuovendo al contempo lo sviluppo economico. La legislazione dell'Unione europea in questo settore si è moltiplicata rapidamente negli anni, utilizzando le basi giuridiche e gli strumenti tipici del mercato interno, per rafforzarne il funzionamento, in un percorso ideale che va dalla Direttiva 2000/31/CE dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare del commercio elettronico, nel mercato interno ("Direttiva sul commercio elettronico"), finalizzata a promuovere lo sviluppo del commercio *online* in un periodo in cui *internet* era ancora agli inizi e la fiducia dei consumatori nelle transazioni via *web* era molto bassa, all'adozione del Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce norme armonizzate sull'intelligenza artificiale ("AI Act"). Molti gli atti che hanno segnato questo percorso: dal Regolamento (UE) 2018/302 del 28 febbraio 2018, relativo alla prevenzione del *geoblocking* ingiustificato e di altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti all'interno del mercato interno, ("Regolamento sul Geoblocking"), alla Direttiva 2010/13/UE sulla coordinazione di determinate disposizioni legislative, regolamentari

[1] Modulo Jean Monnet dal titolo: EU inte(lligent)rnal market between new challenges and old obstacles Finanziamento della Commissione europea: Call for Proposals 2024 ERASMUS-JMO-2024-HEI-TCH-RSCH, Proposal number:101176197.

o amministrative degli Stati membri concernenti la fornitura di servizi di media audiovisivi ("Direttiva sui servizi di media audiovisivi"), modificata dalla Direttiva (UE) 2018/1808 del 14 novembre 2018, dalla Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019, relativa ad alcuni aspetti dei contratti di fornitura di contenuti e servizi digitali al Regolamento (UE) 2022/2065 del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la Direttiva 2000/31/CE ("Digital Services Act") e al Regolamento (UE) 2022/1925 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 ("Digital Markets Act").

Nel rafforzare il mercato interno regolamentando l'utilizzo delle nuove tecnologie e affrontando i nuovi ostacoli da queste sollevati, gli strumenti di diritto dell'Unione hanno altresì perseguito l'obiettivo di tutelare i diritti fondamentali e i valori propri dell'Unione. L'impatto delle nuove tecnologie sul mercato interno e le soluzioni adottate dalla legislazione per fare fronte alle sfide che pone tale rapida evoluzione del mercato interno sono stati al centro delle relazioni dei prestigiosi relatori della *Summer School*, cui è seguito un dibattito con gli studiosi presenti in aula. Il presente numero speciale di *Eurojus* raccoglie alcuni di questi importanti contributi.

Nell'aprire i lavori della *Summer School*, il dott. Salvatore D'Acunto, capo unità, DG Mercato interno, ha ricordato che il Mercato unico resta a tutt'oggi il fulcro dell'integrazione, della crescita e della prosperità economica dell'Unione europea, pur essendo necessario un intervento per rilanciarlo: i rapporti Letta e Draghi del 2024 hanno sottolineato l'urgenza di rimuovere le troppe barriere che ancora sussistono e alcuni studi hanno evidenziato come il potenziale di crescita del PIL europeo toccherebbe livelli molto significativi ove tali ostacoli fossero effettivamente eliminati. La nuova Strategia per il Mercato unico, adottata dalla Commissione europea il 21 maggio 2025 va in questa direzione, proponendo diverse azioni per la rimozione degli ostacoli tuttora esistenti. Il prof. Nascimbene ha proseguito idealmente il percorso di indagine illustrando la progressiva realizzazione del Mercato unico digitale non mancando di evidenziarne il ruolo come nuova prospettiva dell'integrazione europea.

Durante la *Summer School* grande attenzione è stata dedicata al tema della tutela e della circolazione dei dati nel mondo digitale. Il contributo del prof. Vittorio Bachelet analizza la disciplina delle clausole abusive nei

contratti tra imprese introdotta dall'art. 13 del Regolamento (UE) 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828 ("Data Act"), applicabile dal 12 settembre 2025, nel quadro del diritto privato regolatorio europeo. La disciplina, ispirata alla Direttiva 93/13/CEE sulle clausole abusive nei contratti con i consumatori, tutela le imprese contro l'imposizione unilaterale, da parte di altre imprese, di clausole abusive relative all'accesso e all'uso dei dati. Inserita in un regolamento che considera i dati quali beni dotati di valore economico – alla luce del dibattito sull'ammissibilità dello scambio di dati personali contro servizi – essa si colloca nel più ampio quadro della strategia europea dei dati, volta a correggere le asimmetrie del mercato digitale e a promuovere un utilizzo dei dati più equo ed efficiente. Il prof. Marco Orofino ha concentrato la propria analisi sulla circolazione dei dati, dimostrando che il quadro giuridico europeo in materia di dati ha subito una profonda trasformazione: da un modello difensivo incentrato sulla protezione dei dati personali, a un approccio basato sulla *governance* in cui la circolazione dei dati è attivamente promossa in condizioni regolamentate.

Un altro tema ampiamente analizzato e discusso è stato quello dell'impatto delle nuove tecnologie sulla tutela dei diritti fondamentali. Il contributo del prof. Giovanni Ziccardi si concentra sull'analisi del c.d. *deep fake*, analizzando i rischi che si presentano nella società attuale, ove la velocità della comunicazione supera di gran lunga la capacità di verificarne la veridicità, e le tutele offerte dal vigente quadro normativo.

L'attenzione è stata poi dedicata alle prospettive del Mercato Unico Digitale al di là dei confini europei. Il prof. Federico Ferri ha esaminato la dimensione esterna del Mercato Unico Digitale, attraverso l'analisi delle relazioni commerciali (ma non solo) tra Unione europea e Stati terzi. La d.ssa Paulina Kowalicka ha poi concentrato la propria attenzione sui modelli indiano e sudamericano di sviluppo dell'intelligenza artificiale, evidenziandone criticità e pregi.

L'*Ai Act* è stato poi al centro delle analisi e delle discussioni di gran parte delle giornate della *Summer School*, stante la novità di questa legislazione e l'impatto in crescita esponenziale di questa nuova tecnologia. Il contributo del prof. Mario Carta e del dott. Marco Guidi si concentra sul ruolo del *risk-based approach* di questa legislazione, anche con un confronto con il GDPR.

Infine, le relazioni della *Summer School* sono state dedicate all'impatto delle nuove tecnologie sulla tutela della concorrenza. Particolare attenzione è stata dedicata al *Digital Market Act* come nuovo paradigma per la politica di concorrenza dell'UE nei mercati digitali, tra regolamentazione e diritto *antitrust*: a questo tema è dedicato il contributo del prof. Francesco Rossi Dal Pozzo e del dott. Marco Guidi.

Come noto, il mercato interno è un obiettivo in perenne realizzazione, richiedendo un aggiornamento costante per adattarsi alle nuove sfide. Nel corso della pubblicazione di questo numero speciale, molte delle norme oggetto di studio sono state poste in discussione nelle due proposte di regolamento, COM(2025) 837 e COM(2025) 836, presentate congiuntamente nell'ambito del c.d. pacchetto "Digital Omnibus". Occorre pertanto monitorare questo iter legislativo per comprendere le possibili modifiche delle regole europee determinate (anche ma non solo) dall'evolversi della situazione geopolitica. Lo studio delle eventuali modifiche delle norme proseguirà nella prossima edizione della *Summer School* che si terrà nei prossimi giugno-luglio 2026 (le relazioni del presente fascicolo sono aggiornate al 30 settembre 2025).

F. ROSSI DAL POZZO e I. ANRÒ

Il Mercato unico dell'Unione europea: origini, strumenti e sviluppo[*]

di SALVATORE D'ACUNTO[**]

SOMMARIO. 1. Cenni introduttivi. – 2. Le quattro libertà fondamentali del Mercato unico. – 3. I servizi della società dell'informazione all'origine del Mercato Unico Digitale. – 4. Il controllo dell'applicazione delle regole del Mercato unico. – 5. Brevi riflessioni conclusive.

1. Cenni introduttivi

Sono particolarmente grato e onorato di dare il calcio di inizio a questa *Summer School* con la lezione introduttiva, il cui obiettivo è di ricostruire per grandi linee le origini, gli strumenti e lo sviluppo del Mercato unico, all'interno del quale si è man mano affermata e si sta costantemente espandendo la dimensione digitale.

Desidero complimentarmi con gli organizzatori per la tempestività della loro scelta, sia per quanto riguarda i temi affrontati che il contesto anche istituzionale nel quale si iscrive la *Summer School.*

In effetti, appena due settimane prima del suo inizio previsto il 5 giugno 2025, e cioè il 21 maggio 2025, la Commissione europea ha adottato l'attesa nuova Strategia per il Mercato Unico, rispondendo ad una richiesta avanzata da ambiti istituzionali, da varie parti interessate e da personalità autorevoli (vedi rapporti Letta e Draghi) per un rilancio dell'idea e delle ambizioni del nostro progetto di area libera ed integrata al suo interno, come volano di competitività e crescita economica dell'Unione europea.

L'idea di uno spazio comune è sempre stata un obiettivo dinamico, in costante divenire, da conseguire, piuttosto che una realtà statica e assodata. La Strategia di maggio 2025 è solo l'ultima tappa, in ordine di tempo, di un graduale processo di integrazione del Mercato unico, per cogliere il

[*] Il contributo non è stato sottoposto a revisione tra pari, in conformità alle politiche editoriali della *rivista* e nel rispetto dei criteri ANVUR di cui all'art. 2, comma 2, lett. c).

[**] Capo unità presso la Commission europea, Direzione generale del Mercato interno, dell'industria, dell'imprenditoria e delle PMI (GROW), unità *Enforcement*. Le opinioni espresse dall'autore non coincidono necessariamente con quelle della sua Istituzione di appartenenza.

quale occorre ovviamente partire dalle origini, richiamando alcuni passaggi storici e iniziando con la definizione di base che si ritrova nell'articolo 26, par.2, del Trattato sul Funzionamento dell'Unione europea (TFUE), che recita: «il mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali…».

Il primo grande cantiere di realizzazione del Mercato unico fu quello che la Commissione avviò attraverso il Libro bianco del 1985 e che fu poi fatto proprio dal Consiglio europeo di Milano del 1986, il quale, sulla base del famoso rapporto Cecchini sul "Costo della non-Europa", stabilì l'obiettivo di eliminazione delle barriere fisiche, tecniche e fiscali soprattutto in materia di libera circolazione delle merci, attraverso quasi 300 direttive.

Altri momenti salienti sul piano politico sono stati rappresentati dall'Agenda di Lisbona del 2000, che si proponeva di imprimere una scossa decisiva per la crescita dell'economia europea a livello globale, il Piano d'azione del 2020 e, da ultimi, la comunicazione sui trent'anni del Mercato unico del 2023 (che richiama la scadenza 1993, fissata dal Consiglio di Milano) e, appunto, la nuova Strategia del 21 maggio 2025.

Questo dimostra, in positivo, come la realizzazione del Mercato unico abbia rappresentato e continui a restare una priorità fondamentale dell'azione della Commissione, ma, allo stesso tempo, denota pure dei ritardi cronici da colmare con rinnovati impegni e programmi politici.

2. Le quattro libertà fondamentali del Mercato unico

Per comprendere la nozione di Mercato unico, bisogna partire dalle basi, cioè dai tratti essenziali di ognuna delle quattro libertà fondamentali che lo contraddistinguono.

Anzitutto, la libera circolazione delle merci, prevista dagli articoli 28-37 del TFUE, che sanciscono il divieto tanto dei dazi doganali (una nozione tornata prepotentemente in voga negli ultimi tempi) quanto delle restrizioni quantitative o di qualsiasi misura di effetto equivalente, sia all'importazione che all'esportazione di merci. In base alla famosa sentenza Cassis de Dijon del 1979, questa libertà comporta non solo il divieto di discriminazioni ma anche di misure indistintamente applicabili, fermo restando la possibilità di deroghe dovute o a discriminazioni giustificate da eccezioni espressamente previste dal Trattato (quali l'ordine pubblico, la sicurezza o la salute pubblica) o da ulteriori ragioni imperative di interesse generale ammesse dalla giurisprudenza della Corte di giustizia

(come la tutela dell'ambiente o dei consumatori).

In secondo luogo, la libera circolazione delle persone. Essa si articola in due rami principali: la libera circolazione dei lavoratori (articoli da 45 a 48 TFUE) e la libera circolazione dei cittadini dell'UE, disciplinata dalla Direttiva 2004/38, la quale contempla il diritto d'ingresso e di soggiorno fino a tre mesi, il diritto di soggiorno superiore a tre mesi a fronte di risorse economiche e previdenziali sufficienti o evidentemente di attività economiche e professionali o di ragioni di ricongiungimento familiare, e infine il diritto di soggiorno permanente (dopo una residenza legale di cinque anni).

In terzo luogo, la libera circolazione dei capitali. A differenza delle altre, non è stata direttamente applicabile fin dalle origini ma lo è diventata soltanto a seguito della Direttiva 88/361, che ha liberalizzato i movimenti di capitali non solo all'interno dell'Unione ma anche con Stati terzi. Prevista dagli articoli da 63 a 66 TFUE, questa libertà si articola non solo nel divieto di restrizioni ai movimenti di capitali ma anche nella esclusione di ostacoli ai pagamenti tra Stati membri, cioè a quelle operazioni finanziarie che vengono svolte a titolo di controprestazioni di forniture di beni o servizi.

Infine, la libera circolazione dei servizi, intesa *lato sensu* e quindi inclusiva anche della libertà di stabilimento. Si tratta della libertà che, da residuale che era inizialmente, secondo quanto previsto dal trattato di Roma[1], è diventata di fatto la più rilevante, in quanto i servizi coprono ormai praticamente 3/4 della nostra economia. Contemplate rispettivamente degli articoli da 49 a 55 e da 56 a 62 TFUE, la libertà di stabilimento e la libera circolazione dei servizi sono dei principi di applicabilità diretta che conferiscono dei diritti ben precisi ai loro beneficiari, di cui quest'ultimi possono avvalersi nei confronti di autorità statali centrali e locali.

La giurisprudenza della Corte ha, nei decenni, elaborato una interpretazione estremamente estensiva e dinamica di queste libertà. Due esempi su tutti. Anzitutto di queste libertà beneficiano non solo gli operatori economici ma anche i destinatari di servizi, quali turisti, pazienti, studenti, spettatori TV, utenti *online*. E poi la libera circolazione di servizi può essere esercitata, al di là della lettera del Trattato di Roma e grazie

[1] Art.57 TFUE: «sono considerate come servizi le prestazioni fornite normalmente dietro retribuzione, in quanto non siano regolate dalle disposizioni relative alla libera circolazione delle merci, dei capitali e delle persone».

proprio alla interpretazione dinamica della Corte, secondo quattro modalità distinte: spostamento congiunto del prestatore e del cliente da uno Stato membro all'altro, movimento del solo prestatore, dislocazione del solo destinatario e infine trasferimento transfrontaliero del solo servizio, senza movimento di alcune delle parti. E proprio quest'ultima modalità assume una rilevanza specifica per la dimensione digitale del Mercato unico, in quanto i servizi *online* sono per definizione forniti senza spostamento fisico di prestatore o destinatario.

Al di là del Trattato e della relativa giurisprudenza della Corte, il legislatore europeo ha sempre riservato un'attenzione particolare alla disciplina normativa di servizi e stabilimento. Volendo oltremodo semplificare, si possono identificare tre grossi filoni legislativi: uno settoriale, che ha nei decenni regolamentato aree ben precise (quali servizi finanziari, energia, gas, servizi postali, telecomunicazioni, TV, trasporti, ecc.); uno dedicato al riconoscimento delle qualifiche professionali, in cui spicca la Direttiva 2005/36; infine la Direttiva servizi, ribattezzata "Bolkestein" dal nome del commissario che la elaborò in seno alla Commissione Prodi nel 2004. Questa direttiva ha, in qualche modo, fatto la storia non solo dei servizi ma, più in generale, considerata l'estrema complessità del negoziato e anche la viva partecipazione delle categorie interessate (perfino con manifestazioni di massa in piazza nella primavera del 2005), anche sul piano della politica legislativa. Le accese discussioni che portarono alla sua adozione hanno rappresentato una sorta di monito nella preparazione di nuove iniziative molto ambiziose anche negli anni a venire.

Sta di fatto che la Direttiva servizi, che da alcune parti si volle non solo ridimensionare ma praticamente azzerare nei suoi contenuti essenziali, ha invece mostrato una vitalità e una potenzialità che ancora oggi si cerca di cogliere appieno come volano essenziale di rilancio della competitività e della economia europea. Se i servizi rappresentavano nel 1970 soltanto il 45% del PIL, oggi essi raggiungono il 70/75% di esso, a dimostrazione della loro centralità nella creazione di ricchezza e di occupazione. Al contempo, l'integrazione dei servizi a livello transfrontaliero resta inferiore rispetto a quelle delle merci e la maggior parte delle vigenti barriere sono identiche a quelle del 2000, cioè un quarto di secolo fa. Non a caso si lamenta, in modo ricorrente, una debolezza strutturale dell'economia dei servizi dovuta alla scarsa informazione sulle regole applicabile, alla complessità delle procedure di autorizzazione e

certificazione, ai requisiti eccessivamente vincolanti in materia di distacco dei lavoratori o ancora in tema di fiscalità. Tra i settori a bassa mobilità transfrontaliera vengono segnalati la costruzione, la grande distribuzione, i *business services* e il turismo.

Per tornare alla Direttiva servizi, la sua visione e lungimiranza sono state tra l'altro dimostrate dal fatto che essa è stata fonte di ispirazione di altri atti normativi anche a beneficio dei consumatori europei, quali la Direttiva sui diritti dei pazienti 2011/24 o il Regolamento cosiddetto *Geoblocking,* 2018/302, che dà attuazione al divieto di discriminazione in base al luogo di residenza di un acquirente, segnatamente nella dimensione *online*.

3. I servizi della società dell'informazione all'origine del Mercato Unico Digitale

Uno dei principi fondamentali previsti nella proposta originaria della Direttiva servizi era quella del principio del paese d'origine, in base al quale un prestatore qualificato nel suo paese di provenienza non può subire restrizioni relative alle sue attività da parte di un paese di destinazione. Questa regola, che, in quanto tale, non esiste più nella versione finale della Direttiva servizi, è invece presente e viva e vegeta nell'atto fondante del Mercato Unico Digitale: la Direttiva sul commercio elettronico 2000/31, che prevede il principio del paese d'origine nel suo art. 3.

Se da un punto di vista storico la Direttiva sul commercio elettronico ha definito la regolamentazione di base del Mercato Unico Digitale, in realtà tale direttiva riprende un concetto cardine per la dimensione *online*, introdotto un paio di anni prima: si tratta della nozione di "servizi della società dell'informazione" coniata dalla Direttiva "notifiche" 98/48 (ora codificata, assieme alla Direttiva 98/34, nella vigente Direttiva 2015/1535). I servizi della società dell'informazione sono definiti da tre caratteristiche fondamentali e distintive: essere forniti a distanza, per via elettronica e su richiesta individuale di un destinatario. Questa definizione ormai quasi trentennale resta, ad oggi, ancora pienamente applicabile.

Evidentemente il Mercato Unico Digitale è stato caratterizzato da altri fondamentali atti normativi più recenti quali: la Direttiva *copyright* 2002/2065 a tutela di determinati contenuti protetti; il Regolamento (UE) 2022/1925 sui mercati digitali (il *Digital Market Act*), che definisce la responsabilità delle piattaforme di accesso alla dimensione *online*; il Regolamento (UE) 2022/2065 sui servizi digitali (il *Digital Services Act*), che stabilisce regole di trasparenza, responsabilità, diligenza, moderazione

e rimozione di contenuti per determinati prestatori; o ancora il più recente Regolamento (UE) 2024/1689 sull'intelligenza artificiale , che prevede alcune regole in base al rischio nonché una serie di norme in materie di protezione e circolazione dei dati.

4. Il controllo dell'applicazione delle regole del Mercato unico

Il funzionamento e il progresso del Mercato unico sono determinati non soltanto dall'opera del legislatore (Parlamento europeo e Consiglio), che introduce nuove regole, o dall'azione costante di interpretazione giurisprudenziale della Corte di giustizia. L'evoluzione concreta del nostro spazio comune senza frontiere interne è il frutto anche dell'azione svolta dall'istituzione che, in quanto custode del Trattato e del diritto euro-unitario, deve garantire il rispetto delle norme vigenti. Tale ruolo incombe alla Commissione europea, che vigila sull'applicazione del diritto dell'Unione, in generale, e, quindi, del diritto del Mercato unico, in particolare. È un ruolo esclusivo che le spetta insieme a quello di iniziativa legislativa, di potere esecutivo e di rappresentanza esterna dell'UE.

Onde poter svolgere efficacemente questa missione, la Commissione deve innanzitutto essere posta a conoscenza di eventuali violazioni da correggere: lo può fare spontaneamente, d'ufficio, o attraverso dei meccanismi istituzionali, quali la succitata Direttiva notifiche 2015/1535 e il controllo del recepimento corretto delle direttive, o anche attraverso altre fonti di informazione quali pubblicazioni, studi, rapporti, organi di stampa, reclami di cittadini e imprese, ecc.

Per dare un'idea, il numero di progetti normativi nazionali che viene ricevuto a Bruxelles ai sensi della suddetta Direttiva notifiche si aggira ogni anno tra gli 800 ed i 1000 (il Belgio è in testa a questa classifica). Per quanto riguarda, invece, i reclami da parte di cittadini e imprese, attualmente ce ne sono più di 3500 pendenti in tutta la Commissione (l'Italia spicca come il primo paese all'origine di tali segnalazioni). Solo una parte minoritaria, praticamente il 5%, delle denunce sfocia in azioni successive di *enforcement* da parte dell'esecutivo comunitario sotto forma di procedure di infrazione.

Ad ogni buon conto, prima di mettere mano a una procedura di infrazione ai sensi dell'art. 258 TFUE, la Commissione dispone di un ventaglio di strumenti precontenziosi attraverso i quali instaura un dialogo informale con gli Stati. Si tratta di interlocuzioni che possono svolgersi a livello collettivo, per esempio attraverso la SMET, la *Single Market*

Enforcement Task Force[2], o in modo bilaterale mediante lettere amministrative firmate da alti dirigenti o lettere politiche inviate da un Commissario su questioni più sensibili e urgenti. Altri meccanismi di intervento sono rappresentati da SOLVIT[3], capace di risolvere più dell'80% dei casi individuali segnalati nel sistema, o anche le cosiddette procedure *EU-Pilot/Dialogue*, che servono a instaurare una interlocuzione informale ma strutturata tra gli uffici della Commissione e le autorità nazionali.

Tuttavia, quando si parla di *enforcement* il pensiero va immediatamente e inesorabilmente alle procedure di infrazione, che rappresentano lo strumento classico per conseguire l'obiettivo non di tradurre uno Stato davanti alla Corte di giustizia ma di rimuovere un ostacolo al Mercato unico. E ci si riesce nel 95% dei casi senza ricorso giurisdizionale.

Come noto, la procedura di infrazione si articola in tre fasi (lettera di costituzione in mora, parere motivato e ricorso in Corte di giustizia), in cui vengono sollevati determinati addebiti di incompatibilità col diritto UE nei confronti di uno Stato membro: tali doglianze devono essere chiaramente ed esaustivamente individuate fin dall'inizio con la possibilità di farne decadere alcune ma non di aggiungerne altre nel prosieguo della procedura. Ogni decisione di avviare, proseguire o archiviare una procedura di infrazione è un atto che richiede una presa di posizione formale da parte del collegio dei commissari, cioè dell'istituzione in quanto tale.

Si tratta di procedure che possono durare a lungo, anche cinque anni o più, e che non portano a nessuna sanzione (tranne nei casi di mancata comunicazione delle misure nazionali di attuazione di una direttiva, ai sensi dell'art.260, par.3, TFUE). Perché scatti una conseguenza finanziaria nei confronti di un Paese è necessario una seconda sentenza di condanna da parte della Corte di giustizia nei confronti di uno Stato membro che non abbia ottemperato al dispositivo di una prima pronuncia da parte dei giudici di Lussemburgo. La seconda sentenza può far scattare delle sanzioni estremamente onerose sul piano finanziario e l'importante novità rilevante rispetto alla lettera del Trattato all'art. 260, par. 2, TFUE, risiede nel fatto che la Corte ha sancito che essa può comminare non solo la

[2] Si veda: The Single Market Enforcement Taskforce - European Commission.
[3] Si veda: SOLVIT – EU rights problem solving when working, living or doing business in another EU country - European Commission.

sanzione consistente in una somma forfettaria oppure una penalità ma ha facoltà di irrogare cumulativamente (e non solo alternativamente) entrambe nei confronti dello Stato condannato. Sia la somma forfettaria che la penalità possono ammontare a svariate decine di milioni, il che rappresenta un deterrente estremamente incisivo e convincente per gli Stati membri per decidersi ad ottemperare.

Solo a titolo indicativo, ci sono attualmente in Commissione circa 1500 procedure di infrazione pendenti e, di media, ogni Stato membro ha un pacchetto di una cinquantina abbondante di casi, fermo restando che, trattandosi di una media, varia dai 31 *dossier* della Lituania ai 90 della Spagna, poste alle due estremità della classifica.

E, giusto per completare questa panoramica sugli strumenti di applicazione delle regole del Mercato unico, è opportuno anche richiamare i rinvii alla Corte di giustizia di Lussemburgo a titolo di interpretazione pregiudiziale effettuati dalle giurisdizioni nazionali. In questa classifica primeggia la Germania, seguita dall'Italia.

A titolo esemplificativo, si possono individuare cinque grosse categorie di infrazioni su alcune tematiche particolarmente problematiche in tema di Mercato unico: alcune regole e pratiche nazionali in ambito di appalti pubblici e concessioni (si rilevano, in effetti, frequentemente casi di attribuzione diretta di contratti o di modifiche di concessioni senza gara); le folte restrizioni ai servizi e alla libertà di stabilimento (in tema, ad esempio, di autorizzazioni per lo svolgimento di determinate attività economiche in ambito turistico, di grandi distribuzione, di costruzione, ecc.); le professioni regolamentate (ce ne sono circa 5700 in tutta l'Unione), per le quali, benché la stragrande maggioranza dei titoli venga riconosciuta a livello transnazionale, rimangono dei casi ancora numerosi in cui tale riconoscimento o non avviene o è eccessivamente lento e burocratico; i diffusi ostacoli alla libera circolazione delle merci, derivanti, segnatamente, dalle divergenti etichettature nazionali sui prodotti; i molteplici casi di ritardo di pagamento da parte delle pubbliche amministrazioni nazionali, regionali o locali nei confronti di imprese fornitrici di beni e servizi (il che può determinare gravi problemi di liquidità finanziaria per le società e in particolare per le PMI, e in alcuni casi rivelarsi esiziali per la loro sopravvivenza).

5. Brevi riflessioni conclusive

In conclusione, il Mercato unico resta, tutt'oggi, il fulcro dell'integrazione, della crescita e della prosperità economica dell'Unione

europea. I rapporti Letta e Draghi del 2024 hanno sottolineato l'urgenza di rimuovere le troppe barriere che ancora sussistono e alcuni studi hanno evidenziato come il potenziale di crescita del PIL europeo toccherebbe livelli molto significativi ove tali ostacoli fossero effettivamente eliminati: si parla di cifre attorno ai 300/400 miliardi di Euro l'anno, solo per i servizi o di più di tre 700 milioni l'anno, coprendo beni e servizi[4].

Nella strategia adottata lo scorso 21 maggio 2025, la Commissione ha avanzato alcune proposte in tema di: semplificazione degli oneri per le imprese; introduzione di un 28º regime comune per il diritto delle società; uso più esteso dei meccanismi preventivi di valutazione di ostacoli normativi nazionali alla libera circolazione; preferenza per i regolamenti sulle direttive onde conseguire una uniformità legislativa maggiore; necessità di un *enforcement* più incisivo e, quindi, di un uso più diffuso, sistematico e strategico delle procedure di infrazione.

Ma quello che conta sottolineare è, al di là del dato politico, economico e giuridico, che il concetto di Mercato unico deve essere assorbito e fatto proprio dagli Stati membri. La realizzazione del nostro spazio comune, cioè, non è solo un affare di Bruxelles ma una missione che deve essere sentita e condivisa da ogni singolo Stato membro e, per di più, non solo nelle capitali ma nelle oltre 100.000 unità amministrative locali che ci sono a livello UE. Usando proprio il linguaggio digitale, sussiste oggettivamente una sorta di *gap* di "riconoscimento facciale" del Mercato unico: la Direzione generale GROW esiste a Bruxelles in seno all'amministrazione europea ma, a differenza dei dicasteri classici quali agricoltura, trasporti, ambiente, industria, ecc., non esiste negli ordinamenti nazionali il ministero del Mercato unico!

Il Mercato unico, oltre che uno spazio di libera circolazione, è anche e soprattutto un patrimonio di integrazione, di tolleranza e anche un modello economico e sociale proiettato verso l'esterno che continua costantemente ad attirare nuovi candidati. Ci sarà una ragione…

Al di là del valore dei 18.000 miliardi di Euro del Mercato unico o del fatto che esso rappresenta il 18% del PIL mondiale e 56 milioni di posti di lavoro, è necessario che questo progetto comune europeo e questa visione condivisa di crescita economica e di protezione dei nostri valori fondamentali siano sempre più sentiti e difesi non solo a Bruxelles ma in

[4] Si veda, European Parliamentary Research Service, *Completing the single market for services*, 2022. Si veda, altresì, European Parliament Research Service, *Mapping the Cost of Non-Europe 2019-2024*, Study of the European Parliament Research Service, 2019.

tutto il territorio dell'Unione, da ogni autorità nazionale, da ogni impresa e da ogni cittadino come un'identità propria.

Il Mercato Unico Digitale è una nuova frontiera dell'integrazione europea?

di BRUNO NASCIMBENE [*]

SOMMARIO. 1. Introduzione. – 2. Le domande. Le norme rilevanti. – 3. La "specialità" del Mercato digitale. I diritti fondamentali e la protezione dei dati personali. – 4. La realizzazione progressiva. – 5. Una nuova frontiera dell'integrazione? Lo spazio digitale. – 6. Le azioni chiave. La realizzazione della prima agenda digitale. I tre pilastri. – 7. La seconda agenda digitale. Il decennio 2020-2030. Gli obiettivi (tre). – 8. Gli atti più importanti del decennio. – 8.1. Il mercato dei servizi. – 8.2. Il mercato e la concorrenza. La necessità di una regolamentazione *ex ante*. – 8.3. L'intelligenza artificiale. – 9. Alcune conclusioni possibili. – 9.1. Le conseguenze della transizione digitale. – 9.2. La convergenza multimediale. – 9.3. La tutela dei diritti fondamentali. – 9.4. L'applicazione del DMA e il ruolo della Commissione.

1. Introduzione

Il titolo di questo intervento introduttivo al corso della *Summer School* 2025 trae spunto da un breve scritto pubblicato nel 2020, in un numero speciale di *eurojus*, a cura di Francesco Rossi Dal Pozzo, dal titolo *Mercato unico digitale, dati personali e diritti fondamentali*[1].

Ne riprendo solo alcuni punti essenziali, il tempo trascorso ha inciso in modo rilevante sul tema; l'intervento, peraltro, è solo introduttivo rispetto alla molteplicità di argomenti che sono oggetto del corso[2].

---

[*] Già professore ordinario di diritto internazionale, professore emerito di diritto dell'Unione europea presso l'Università degli Studi di Milano.

[1] Si veda il fascicolo speciale, luglio 2020, https://rivista.eurojus.it/mercato-unico-digitale-dati-personalie-diritti-fondamentali/; il titolo del contributo, p. 11 ss. è *Il mercato unico digitale quale nuova frontiera.dell'integrazione europea. Considerazioni introduttive*.

[2] Considerata la natura del presente lavoro, le indicazioni bibliografiche hanno carattere essenziale e sono indicate secondo i rispettivi paragrafi: "1. Introduzione", v. K. WECKSTRÖM LINDROOS, M.L. MONTAGNANI, K. KLAFKOWSKA-WAŚNIOWSKA, A. MICKIEWICZ (a cura di), *Governance of Digital Single Market Actors,* Northampton, 2025; R. TORINO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023. "2. Le domande. Le norme rilevanti", v. G. ALPA, *Il mercato unico digitale*, in *Contratto e impresa Europa*, 2021, p. 1 ss.; F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali* cit.; C. BURY, I. R. LAGUNA, *'Tinkering or Fundamental*

2. Le domande. Le norme rilevanti

Le domande che si pongono sono molte, a cominciare proprio dal titolo che è, invero, una domanda, e che si riferisce al concetto di mercato "unico", ovvero al mercato "interno", nel passato definito "comune": qualificazioni, queste, equivalenti, il cui riferimento normativo, rinvenibile nell'art. 3, par. 3 TUE ("L'Unione instaura un mercato interno") e nell'art.

Overhaul?' The Past, the Present ad the Future of the Digital Single Market, in S. GARBEN, I. GOVAERE (a cura di), *The Internal Market 2.0*, Oxford, 2020, p. 235 ss.. "3. La "specialità" del mercato digitale. I diritti fondamentali e la protezione dei dati personali", v. A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE – Sezione "Atti convegni AISDUE"*, n. 15/2023, p. 321 ss.; M. SANTANIELLO, *Sovranità digitale e diritti fondamentali: un modello europeo di Internet governance*, in *Rivista italiana di informatica e diritto*, 2022, p. 47 ss.; F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale,* Torino, 2022; B. NASCIMBENE, *Carta dei diritti fondamentali, applicabilità e rapporti fra giudici: la necessità di una tutela integrata*, in *European Papers*, 6/2021, p. 81 ss.; O. POLLICINO, *Tutela dei diritti fondamentali nell'era digitale e contesto valoriale: una indagine transatlantica*, in *MediaLaws – Rivista di diritto dei media*, 2018, p. 39 ss.; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* Safe Harbour *al* Privacy Shield), in *Rivista di diritto internazionale*, 2016, p. 690 ss.. "4. La realizzazione progressiva", v. I. GOVAERE, S. GARBEN (a cura di), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford, 2017; U. PAGALLO, *The Legal Challenges of Big Data: Putting Secondary Rules First in the Field of EU Data Protection*, in *European Data Protection Law Review*, 2017, p. 36 ss.; N. TSAGOURIAS, R. BUCHAN (a cura di), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015. "5. Una nuova frontiera dell'integrazione? Lo spazio digitale", v. R. CAVALLO PERIN, D. U. GALETTA (a cura di) *Il diritto dell'amministrazione pubblica digitale*, Torino, 2025; F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *Il Diritto dell'Unione Europea*, 2022, p. 277 ss. "6. Le azioni chiave. La realizzazione della prima agenda digitale. I tre pilastri", v. G. GONZÁLEZ-FUSTER, R. VAN BRAKEL, P. DE HERT (a cura di) *Research Handbook on Privacy and Data Protection Law*, Cheltenham, 2022; G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *Commentario GDPR e Normativa Privacy*, Milano, 2022; M. OROFINO, *La multilevel "governance" delle comunicazioni elettroniche venti anni dopo il Framework 2002*, in *Federalismi.it*, 2022, p. 692 ss.; R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e* data protection, Milano, 2021; G. CAGGIANO, *Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme* online *e tutela dei diritti fondamentali nel quadro del* Digital Service Act *e della co-regolamentazione*, in *Papers di diritto europeo*, 1/2021, p. 45 ss.; R. MASTROIANNI, *La determinazione del* country of origin *ed il principio del mutuo riconoscimento nel nuovo testo della direttiva sui servizi di media audiovisivi*, in *Temi e questioni di diritto dell'Unione europea*, in *Scritti offerti a Claudia Morviducci*, Bari, 2019, p. 167 ss.. "7. La seconda agenda digitale. Il decennio 2020-2030. Gli obiettivi (tre)", v. M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in questa *Rivista*, 3/2024, p. 188 ss.; F. FERRI (a cura di), *La nuova disciplina UE sull'intelligenza artificiale: questioni e prospettive*, in *Quaderni AISDUE – fasc. spec. n. 2*, Napoli, 2024; F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione,* Milano, 2018. "8. Gli atti più importanti del decennio", v. G. MUSCOLO, A. MASSOLO (a cura di), *Navigating The DMA: Application Across National Jurisdictions*, Paris-London-New York, 2025; G. CARATOZZOLO, *The Digital Markets Act in action: analysis of the early practice of the Commission*, in questa *Rivista*, 3/2024, p. 141 ss.; F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023; V. FALCE, *Fairness e innovazione nel mercato unico digitale*, Torino, 2020; A. EZRACHI, *EU Competition Law Goals and the Digital Economy*, Oxford, 2018. "9. Alcune conclusioni possibili", v. R. TORINO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2024; S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *Annali AISDUE – Sezione "Atti convegni AISDUE"*, 5/2021, p. 69 ss.

26 TFUE che insieme all'art. 27 costituisce il titolo I, "Mercato interno", della parte terza del TFUE dedicata alle "Politiche e azioni interne dell'Unione"[3].

Precisa l'art. 26, par. 2, che il "mercato interno comporta uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni dei trattati", conferendo quindi (par. 3) la competenza al Consiglio, su proposta della Commissione, di definire "gli orientamenti e le condizioni necessari per garantire un progresso equilibrato nell'insieme dei settori considerati".

La realizzazione del mercato interno, quale che sia il settore coinvolto, ha una posizione centrale nel processo di integrazione. Una attenzione speciale è dedicata al settore della concorrenza, oggetto di un protocollo *ad hoc* allegato ai trattati (protocollo n. 27 "sul mercato interno e sulla concorrenza"), ove si precisa che ex art. 3 TUE il mercato interno "comprende un sistema che assicura che la concorrenza non sia falsata", ma soprattutto consente (art. 352 TFUE) l'adozione di misure ovvero l'esercizio di poteri di azione non espressamente previsti dai trattati per realizzare l'obiettivo proposto.

Le competenze dell'Unione (come si dirà pure oltre) sono concorrenti con quelle degli Stati, secondo quanto dispone l'art. 4, par. 2, lett. a) TFUE e vengono esercitate per l'instaurazione e il funzionamento del mercato interno, come prevede l'art. 114 TFUE (di cui si dirà pure oltre). Il processo di cui ci occupiamo, nelle sue varie e diverse manifestazioni, una delle quali è il Mercato unico "digitale", è dinamico: l'esame e la valutazione dello stesso richiede un aggiornamento costante, soprattutto quando i settori coinvolti sono quelli della tecnologia, della ricerca e della scienza. Nel maggio del 2015, a riprova di questo dinamismo "intrinseco", la Commissione ha presentato una nuova "Strategia per il mercato unico": un pacchetto, il quarto, denominato omnibus di semplificazione, con l'obiettivo dichiarato di renderlo più semplice, omogeneo e solido, adottando azioni concrete per *a*) eliminare gli ostacoli che ancora frenano la circolazione di beni e servizi tra i Paesi membri, *b*) sostenere le piccole e medie imprese, *c*) promuovere la digitalizzazione e *d*) alleggerire il carico normativo per le imprese. La digitalizzazione, in particolare,

[3] Su questa nozione si rinvia alla relazione nel corso della *Summer School* di S. D'ACUNTO, *Il mercato unico dell'Unione europea: origini, strumento e sviluppo*.

dovrebbe riguardare gli obblighi normativi, consentendo alle imprese di sostituire i documenti cartacei con versioni digitali[4].

3. La "specialità" del Mercato digitale. I diritti fondamentali e la protezione dei dati personali

Il mercato digitale (aggettivo di derivazione latina, da *digitus*, cioè dito, prima ancora che inglese; digital è derivato da digit, cioè cifra di un sistema di numerazione) è una *species* del *genus* mercato interno, una specificazione del generale processo di integrazione e riguarda tutti i settori dell'economia, ne condivide gli obiettivi, fra i quali (art. 3, par. 3), oltre alla "crescita economica equilibrata", la promozione del "progresso scientifico e tecnologico".

Questo rapporto crescita-progresso deve essere sempre tenuto presente, anche per quanto riguarda la tutela dei diritti fondamentali della persona: questa deve essere assicurata in tutte le espressioni e manifestazioni del progresso tecnologico e scientifico. Mi riferisco sia alla Carta dei diritti fondamentali, il cui art. 8 riguarda la "Protezione dei dati di carattere personale" (norma che ha un suo legame con l'art. 8 della Convenzione europea dei diritti dell'uomo), sia all'art. 16 TFUE che prevede il diritto di ogni persona "alla protezione dei dati personali che la riguardano" (facendo salve, ex art. 39 TUE, le norme speciali che il Consiglio può adottare con riguardo al trattamento dei dati da parte degli Stati membri nell'ambito della politica estera e di sicurezza comune).

4. La realizzazione progressiva

La realizzazione progressiva comporta una valutazione nel corso del tempo. Il Mercato unico nasce il 1.1.1993, il mercato digitale, sostanzialmente, nel 2015, quando la Commissione propose una "Strategia per il mercato unico digitale in Europa" (COM [2015] def. del 6.5.2015), che faceva seguito a un documento di qualche anno prima (2010), denominato "Agenda digitale europea"[5] ove si sottolineava il carattere fondamentale ovvero il ruolo chiave delle tecnologie dell'informazione e della comunicazione (TIC) per raggiungere l'obiettivo di un mercato unico in tale settore, caratterizzato ancora da frammentazione e mancanza di interoperabilità.

[4] Si veda la comunicazione del 21 maggio 2025, COM (2025) 500 def. "Il mercato unico: il nostro mercato interno europeo in un mondo incerto. Una strategia per rendere il mercato unico semplice, fluido e forte".
[5] Cfr. il doc. COM (2010) 245 def. del 19 maggio 2010.

Si prendeva atto che il fenomeno del Mercato Unico Digitale era, appunto, trasversale a vari settori: oltre a mercato unico e concorrenza (già ricordati), industria, commercio, reti transeuropee, energia, ricerca, istruzione, cultura.

Avendo riguardo, in particolare, alla libera circolazione di beni e servizi, si è fatto preciso riferimento allo scambio online di beni e servizi, cui i "dati digitali" appartengono. Scambio significa garantire la libera circolazione, senza barriere di carattere normativo, in modo da creare (come afferma la Commissione)[6] un "mercato unico digitale connesso per tutti": una connessione internet per tutti in un contesto in cui deve prevalere un senso di affidabilità e fiducia per imprese e consumatori che sono i soggetti, oltre che i destinatari, di questo mercato.

Il mercato, per essere realizzato, richiede l'armonizzazione delle politiche nazionali, e quindi il ricorso a quella norma (di cui si dirà anche oltre), l'art. 114 TFUE che prevede il "ravvicinamento delle disposizioni legislative, regolamentari e amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno". Se manca la collaborazione fra Stati e istituzioni UE l'innovazione, il progresso tecnologico, la c.d. rivoluzione digitale non si realizzano. La competenza dell'Unione è, d'altra parte, concorrente con quella degli Stati (art. 4, par. 2, lett. a) TFUE) e pertanto gli Stati possono adottare norme solo fino a quando, e quindi nella misura in cui, l'Unione non abbia esercitato la propria competenza legislativa (esercizio della *pre-emption* nell'ambito delle competenze concorrenti).

La strategia prima ricordata è stata attuata (ventinove le iniziative previste); agenzie o organismi sono stati creati (Comitato europeo per la protezione dei dati, Garante europeo per la protezione dei dati, istituiti dal regolamento GDPR, cioè il regol. 679/2016 del 27.4.2016, *General Data Protection Regulation;* Agenzia per la cibersicurezza -Enisa *European Union Agency for Cyber Security*, di cui al Regolamento 2019/881 del 17.4.2019), ma la politica digitale non potrebbe dirsi completata se la Commissione non continuasse a perseguire gli obiettivi previsti sia negli "orientamenti politici" adottati dalla Commissione per il periodo 2019-2024, in particolare la priorità di un'Europa "pronta per l'era digitale", sia quanto previsto in una comunicazione dal significativo titolo "Plasmare il

[6] Cfr. il doc. COM (2017) def. del 10 maggio 2017 sulla "revisione intermedia dell'attuazione del mercato unico digitale".

futuro digitale dell'Europa"[7]. In tale contesto è stata adottata una "*Bussola per il digitale 2030*: *il modello europeo per il decennio digitale*"[8] che ha definito, avendo riguardo al decennio 2020-2030 (e quindi andando oltre la data del 2024 indicata negli "orientamenti" prima ricordati), gli obiettivi digitali dell'Unione per il 2030 in materia di competenze, governo, imprese, infrastrutture.

5. Una nuova frontiera dell'integrazione? Lo spazio digitale

Il Mercato Unico Digitale è (come si è prima detto, ponendo l'interrogativo e rispondendo positivamente) una nuova frontiera dell'integrazione europea, è un mezzo o strumento per realizzarla nel miglior modo possibile a vantaggio di quei soggetti, persone, consumatori, imprese che ne sono i destinatari e beneficiari, e per i quali è stato istituito uno "sportello digitale unico" che consente l'accesso online a informazioni, procedure e servizi di assistenza e di risoluzione dei problemi (Regolamento [UE] 2018/1724 del 2.10.2018 che ha come base giuridica non solo l'art. 114, par. 1 TFUE, ma anche l'art. 21, par. 2 perché riguarda anche la libera circolazione dei cittadini).

I dati, insomma, intesi come *commodities*, devono poter circolare liberamente creando lo spazio digitale che le istituzioni, in una solenne Dichiarazione comune che guarda al futuro (decennio 2020-2030)[9] si sono impegnate a realizzare e garantire. Si tratta di una Dichiarazione che (punto 10) "non incide sul contenuto delle norme giuridiche o sulla loro applicazione", ma che si basa sulle stesse, sul diritto sia primario sia derivato, sulla Carta dei diritti fondamentali, sulla giurisprudenza della Corte di giustizia. L'obiettivo – si afferma nella premessa ai sei capitoli della Dichiarazione – è "promuovere un modello europeo per la trasformazione digitale", con al centro le persone, le imprese, la società nel suo complesso, assicurando la tutela dei diritti fondamentali.

6. Le azioni chiave. La realizzazione della prima agenda digitale. I tre pilastri

Il Mercato Unico Digitale consta di una varietà di misure e di atti, normativi e di *soft law*, riconducibili (almeno per il periodo iniziale) a sedici azioni chiave interdipendenti, raggruppate in tre pilastri: *a*)

---

[7] Cfr. il doc. COM (2020) 67 def. del 19 maggio 2020.
[8] Cfr. il doc. COM (2021) 118 def. del 9 marzo 2021.
[9] Cfr. la "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale", 2023/C 23/01 del 15 dicembre 2022.

migliorare l'accesso *online* dei consumatori e delle imprese ai beni e servizi digitali in Europa; *b*) creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi; *c*) massimizzare il potenziale di crescita dell'economia digitale.

6.1. Riassuntivamente, appartengono al primo pilastro (a favore di consumatori e imprese):

a) sia le misure riguardanti la protezione del diritto d'autore, in particolare i contenuti digitali protetti dal diritto d'autore e la necessità di garantire la "portabilità" degli stessi, quindi la circolazione (poter godere degli stessi contenuti *online*, come film, eventi sportivi, avendo sottoscritto un abbonamento, durante un soggiorno in altro Paese membro della UE);

b) sia le misure sul commercio elettronico, al fine di favorire consumatori e imprese eliminando gli ostacoli derivanti da differenti normative. Le pratiche di geolocalizzazione o *geoblocking* che limitavano l'accesso dei consumatori ad acquisti in funzione della residenza sono state vietate (reg. 2018/32 del 28.2.2018, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell'ambito del mercato interno).

6.2. Riassuntivamente, appartengono al secondo pilastro (a favore dello sviluppo di reti e servizi):

a) le misure in materia di protezione dei dati personali, che devono essere protetti, in quanto diritti fondamentali (tutela della dignità, della riservatezza) non solo nell'ambito dell'Unione, ma anche a livello internazionale. La fiducia nei servizi online deve essere assicurata, garantendo vantaggi sia alle persone, sia alle imprese (sotto il profilo della competitività e del commercio); la norma di maggior rilievo è il regolamento GDPR (già ricordato), cui si accompagna la Direttiva 680/2016 del 27.4.2016 sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia.

b) Al secondo pilastro appartengono inoltre le misure in materia di telecomunicazioni elettroniche. L'atto di maggior rilievo è il Codice europeo delle comunicazioni elettroniche istituito dalla Direttiva 2018/1972 dell'11.12.2018 che armonizza le norme relative all'accesso alle reti, alla concorrenza, ai diritti degli utenti finali. Vengono migliorati reti e servizi come la fibra ottica, il 5G, internet.

Vengono modificati e migliorati i Servizi di Media Audiovisivi (SMA), intervenendo così sulle piattaforme di *video on demand* (come *Netflix*) e

sui servizi di condivisione video (come *YouTube*). L'accesso ai contenuti audiovisivi richiedeva un intervento, avvenuto con la Direttiva 2018/1808 (SMA del 14.11.2018 sul coordinamento di determinate disposizioni legislative, regolamentari e amministrative concernenti la fornitura di media audiovisivi) che ha esteso la precedente disciplina a nuovi mezzi di fruizione dei servizi, come le piattaforme *online*, prevedendo obblighi in materia di tutela dei minori, contrasto ai discorsi d'odio, promozione delle opere europee.

6.3. Riassuntivamente, appartengono al terzo pilastro (crescita dell'economia digitale) le misure che riguardano la circolazione e l'utilizzo di dati non personali (che non permettono, dunque, l'identificazione di una persona fisica): dati statistici, meteorologici, economici, finanziari, sociali, ambientali.

Sono dati che assumono rilievo in tutti i settori dell'economia, ed è stato quindi necessario intervenire prima con una comunicazione ("costruire un'economia dei dati europea") e poi con un regolamento (2018/1807) "relativo a un quadro applicabile alla libera circolazione dei dati non personali", al fine di superare la frammentazione normativa ed eliminare gli ostacoli derivanti dalla localizzazione dei dati[10].

I dati sono indispensabili ad alimentare il funzionamento delle tecnologie digitali, quali gli algoritmi e l'intelligenza artificiale e a promuovere quella trasformazione digitale che riguarda non solo i privati, ma anche la pubblica amministrazione (in tal senso la comunicazione della Commissione sull'accelerazione della trasformazione digitale della pubblica amministrazione, "Piano d'azione dell'UE per l'eGovernment 2016-2020")[11].

7. La seconda agenda digitale. Il decennio 2020-2030. Gli obiettivi (tre)

Alla prima agenda digitale europea, che in sostanza copre il periodo 2010-2020, e che era strutturata sui tre pilastri e sugli atti prima ricordati, è seguita una seconda agenda 2020- 2030, illustrata nella comunicazione della Commissione (prima ricordata) "Plasmare il futuro digitale dell'Europa", pubblicata nel 2020 insieme ad altri due importanti documenti: il *Libro bianco sull'intelligenza artificiale e la Strategia*

[10] Cfr. il doc. COM (2017) 9 def. del 10 gennaio 2017; il regolamento è del 14 novembre 2018.

[11] Cfr. il doc. COM (2016) 179 def. del 19 aprile 2016.

europea dei dati[12]. La Commissione nel 2021 ha adottato un Programma strategico o "Percorso per il decennio digitale"[13], cui seguiva (a fine 2022) la decisione del Parlamento e del Consiglio del 14.12.2022[14] e la "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale" (già ricordata) che rappresenta una sorta di completamento del "Percorso".

La trasformazione digitale, dopo un decennio di positivi risultati raggruppabili, come si è detto, nei tre pilastri, si sviluppa avendo maggiore riguardo ai profili sociali e a quelli economico-sociali, pur sempre nel contesto delle finalità di cui all'art. 3, par. 3, in particolare della "economia sociale di mercato fortemente competitiva", che mira, fra l'altro, alla "piena occupazione e al progresso sociale". Vengono messe al primo posto della trasformazione le persone e, infatti, uno dei tre obiettivi della nuova strategia è sviluppare una tecnologia al servizio delle persone, migliorandone la vita, anche quotidiana, nel rispetto dei diritti fondamentali e dei valori dell'Unione.

Il secondo obiettivo è realizzare un'economia equa e competitiva, a favore delle imprese (quale ne sia la dimensione) e dei consumatori (assicurando il rispetto dei loro diritti).

Il terzo obiettivo è creare una società aperta, democratica e sostenibile, garantendo ai cittadini un ambiente affidabile, con riguardo ai dati che vengono forniti *online* e *offline*, garantendo il rispetto dei valori democratici e il perseguimento di un'economia dinamica e sostenibile (si mira a una trasformazione non solo digitale ma anche verde, ove sia tutelato l'ambiente). Con lo spazio digitale degli anni '20-30, insomma, si vuole migliorare la qualità della vita.

8. Gli atti più importanti del decennio

In questa prospettiva si collocano tre atti importanti: il *Digital Services Act* (DSA), Regolamento 2022/2065 del 19.10.2022, relativo a un Mercato Unico dei servizi digitali, che modifica la Direttiva 2000/31 sul commercio elettronico; il *Digital Markets Act* (DMA) Regolamento 2022/1925 del 14.9.2022, relativo a mercati equi e contendibili nel settore digitale, che

[12] Cfr. il doc. COM (2020) 65 def. del 19 febbraio 2020; il doc. COM (2020) 66 def. del 19 febbraio 2020.
[13] Cfr. il doc. COM (2021) 574 def. del 15 settembre 2021; base giuridica è l'art. 173 TFUE in materia di politica industriale.
[14] Decisione 2022/2481 del 14 febbraio 2022 che istituisce il programma strategico per il decennio digitale 2030.

con il primo costituisce un pacchetto o *package* di provvedimenti; il *AI Act*, Regolamento sull'intelligenza artificiale 2024/1689 del 13.6.2024, che riprende, almeno in parte, il Regolamento generale sulla protezione dei dati GDPR (in tema di responsabilizzazione-*accountability* del fornitore o utilizzatore di sistemi di AI, così come nel quadro del GDPR responsabile è il titolare del trattamento dei dati personali).

8.1. Il mercato dei servizi

Il DSA ha l'obiettivo (art. 1) di "contribuire al corretto funzionamento del mercato interno dei servizi intermediari" (cioè i servizi della società dell'informazione) "offerti a destinatari il cui luogo di stabilimento si trova nell'Unione o che sono ubicati nell'Unione, indipendentemente dal luogo di stabilimento dei prestatori di tali servizi intermediari". Si vuole creare un ambiente *online* più sicuro per i consumatori e le imprese (è una sorta di evoluzione della direttiva sul commercio elettronico che, invero, viene formalmente modificata), prevedendo norme che proteggono i consumatori e quindi definiscono responsabilità a carico dei prestatori di servizi digitali, in particolare le piattaforme digitali e i motori di ricerca di grandi dimensioni. Le norme intendono contrastare sia la diffusione di contenuti illeciti e notizie false o *fake news*, sia la vendita di prodotti contraffatti o pericolosi, sia garantire la trasparenza nella gestione delle informazioni online. Vengono disciplinati obblighi, appunto, e responsabilità dei c.d. intermediari (fra i quali le piattaforme digitali), senza sostituire le norme di settore (per esempio sul diritto d'autore, sulla protezione dei dati personali), prevedendo dunque un quadro generale.

8.2. Il mercato e la concorrenza. La necessità di una regolamentazione *ex ante*

Il DMA è un insieme di norme di condotta per le imprese (c.d. *gatekeeper* o controllori di accessi, come *Microsoft, Meta, Alphabet*) che forniscono servizi di piattaforma di base o essenziali (il regolamento, art. 2, n. 2 elenca dieci servizi, come quelli di intermediazione online, motori di ricerca *online*, pubblicità *online*, assistenti virtuali) che hanno un impatto significativo sul mercato interno, ovvero influiscono sul panorama digitale e, quindi, su milioni di aziende e consumatori), garantendo una concorrenza reale ed effettiva nel mercato digitale. Le norme in questione mirano a integrare l'applicazione del diritto della concorrenza (10° considerando), limitando il potere di alcune grandi piattaforme tecnologiche. Prevedono dunque divieti e prescrizioni, regolando ex ante

le condotte: per esempio l'uso di dati per la pubblicità online, che può avvenire solo con il consenso esplicito dell'utente; il divieto di esclusiva per i commercianti sulla piattaforma; la libertà di scelta per quanto riguarda i *marketplace* (cioè i siti o piattaforme *internet* dedicati alla compravendita di un prodotto o di un servizio, come Amazon); l'interoperabilità e la portabilità dei dati.

Lo scopo di garantire condizioni di mercato eque e competitive si fonda anche sull'esperienza derivante, nel passato (di qui la necessità di norme nuove, utili allo scopo), dal contenzioso instaurato dalla Commissione, poi oggetto di sentenze del Tribunale e della Corte di giustizia che hanno ritenuto incompatibili con l'art. 102 TFUE sull'abuso di posizione dominante quelle pratiche restrittive di operatori attivi nei mercati digitali, come *Google* che ha abusato della propria posizione dominante sul mercato dei servizi di ricerca generale online, nell'ambito del servizio di comparazione dei prodotti (venivano favoriti, attraverso una visibilità privilegiata e, quindi, catturando l'attenzione dell'utente, i risultati provenienti da *Google Shopping*, come ha ritenuto la Commissione, prima, e il Tribunale nonché la Corte di giustizia poi[15]. La visibilità dei servizi concorrenti veniva compromessa, alterando le condizioni di concorrenza, e l'impresa che aveva violato la concorrenza (condotta c.d. *self preferencing*, cioè il trattamento preferenziale per i propri prodotti e servizi) veniva sanzionata.

Altro caso che ha riguardato sempre *Google* e che ha sottolineato la necessità di norme preventive (o *ex ante*) rispetto a comportamenti che ostacolano la concorrenza e l'innovazione (non già successive o ex post come lo strumento antitrust previsto dall'art. 102 TFUE) è rappresentato dalle restrizioni illegittime (restrizioni contrattuali anticoncorrenziali) imposte ai produttori di dispositivi mobili *Android* e agli operatori di reti mobili che, fra l'altro, non potevano usare versioni di *Android* se non quelle approvate da *Google*. Veniva quindi impedito a motori di ricerca concorrenti di *Google* di accedere al mercato sulla base dei propri "meriti" (*Google* imponeva le proprie applicazioni di ricerca generica *Google Search* e di navigazione *Chrome*). *Google* veniva sanzionata, il Tribunale

[15] Cfr. la decisione della Commissione del 27 giugno 2017, *Google Search (Shopping)* e le sentenze del Tribunale UE del 10 novembre 2021, T-612/17, EU:C:2021:763 e della Corte del 10 settembre 2024, C-48/22 P, EU:C:2024:726.

UE confermando, in larga misura, la decisione della Commissione[16].

8.3. L'intelligenza artificiale

Il Regolamento AI 1689/2024, che riprende in parte, come si è detto, il GDPR (prevedendo la responsabilizzazione del fornitore o utilizzatore dei sistemi di AI, come già quella del titolare dei dati personali nel quadro del GDPR) istituisce un quadro giuridico armonizzato per la progettazione, l'immissione sul mercato, la messa in servizio, l'utilizzo di sistemi di intelligenza artificiale, cioè *software*, insieme di istruzioni, dati o programmi o sistemi che sono progettati, utilizzando algoritmi per svolgere compiti che richiedono l'intelligenza umana e, quindi, simulano capacità intellettive umane come quelle di imparare, ragionare, risolvere problemi, prendere decisioni.

Il regolamento (in vigore dal 1.8.2024) applicabile dal 2 agosto 2025 quanto alle norme di governance e obblighi per i modelli di IA per uso generale e dal 2 agosto 2027 per i sistemi di IA ad alto rischio, ha lo scopo di promuovere lo sviluppo e la diffusione responsabile della IA nell'Unione europea, offrendo tutele specifiche alle persone, proteggendo quindi i loro diritti fondamentali.

L'obiettivo, nel quadro della strategia digitale dell'Unione, è di garantire condizioni migliori e di sicurezza giuridica per lo sviluppo e l'uso di una innovativa tecnologia, tenendo conto non solo dei vantaggi e benefici che può apportare (migliore assistenza sanitaria, trasporti più sicuri e puliti, produzione più efficiente, energia più conveniente e sostenibile), ma dei rischi che l'utilizzazione può comportare per gli utenti, e quindi prevedendo obblighi per fornitori e utenti delle tecnologie, a seconda dei livelli (quattro) di rischio: *a*) rischio inaccettabile, e l'applicazione è vietata se i sistemi rappresentano una minaccia per la sicurezza; *b*) rischi minimi o nulli, come i filtri antispam e i giochi; *c*)rischi limitati come i chatbot; *d*) rischi elevati come quelli insiti nella diagnosi delle malattie o nella guida autonoma.

Sanzioni pecuniarie, calcolate sulla base di una percentuale del fatturato (complessivo, realizzato dalla società nell'anno precedente) o su un importo fisso, se superiore (sanzioni proporzionali sono previste per le PMI e le *start-up*) sono previste in caso di violazione delle norme del regolamento.

[16] Sentenza del 14 settembre 2022, T-604/18, *Google e Alphabet c. Commissione*, pendente in Corte, C-738/22 P, conclusioni dell'avvocato generale Kokott del 19 giugno 2025, EU:C:2025:463.

Una delle maggiori difficoltà di queste nuove norme è garantire un'informazione trasparente, garantire misure preventive per limitare possibili danni, bilanciare, dunque, e conciliare la protezione dei diritti delle persone con l'innovazione tecnologica. Come realizzare, insomma, la finalità (prospettata dall'UE) di rendere la vita *online* più facile e più sicura, migliorando l'ambiente digitale. Una "vita digitale" migliore, ma che deve essere sicura e rispettosa dei diritti fondamentali.

9. Alcune conclusioni possibili

9.1. Le conseguenze della transizione digitale

Il fenomeno o transizione digitale ha avuto e continua ad avere delle conseguenze importanti: *a*) sul diritto UE, in generale; *b*) sul mercato unico in particolare, ma *c*) anche sul diritto della concorrenza. Si è ricordato il protocollo n. 27, ma ben si può ricordare anche la comunicazione su "una politica della concorrenza pronta a nuove sfide" che sottolinea lo stretto nesso esistente fra nuove tecnologie e concorrenza[17]. Il fenomeno digitale, come si è detto, è trasversale, riguarda vari settori sia dell'economia, sia del diritto.

9.2. La convergenza multimediale

I confini fra telecomunicazioni, radiodiffusione, tecnologie informatiche (TIC, "Tecnologie dell'informazione e della comunicazione", già ricordate) si sono attenuati nel corso del tempo. Si è creata una convergenza multimediale, ovvero un nuovo spazio tecnologico-digitale in cui si manifesta e realizza la rivoluzione digitale.

9.3. La tutela dei diritti fondamentali

A fronte di questa rivoluzione digitale si osserva che l'uso dei dati digitali ha inciso e incide sulla tutela dei diritti fondamentali della persona, come la Corte di giustizia ha riconosciuto nella sentenza *Digital Rights Ireland*[18] dichiarando invalida la direttiva sulla conservazione dei dati personali ("dati generali o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione", 2006/24/CE del 15.3.2006). La direttiva comportava un'ingerenza di vasta portata che eccedeva i limiti imposti dal rispetto del principio di proporzionalità, alla luce delle norme della Carta che tutelano

[17] Cfr. il doc. COM (2021) 713 def. del 18 novembre 2021.
[18] Corte giust., 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, EU:C:2014:238.

il rispetto della vita privata e la protezione dei dati personali (ingerenza non limitata allo stretto necessario, artt. 7, 8, 52, par. 1 Carta).

9.4. L'applicazione del DMA e il ruolo della Commissione

Un esempio di come possono interagire le norme sulla concorrenza con le norme sul mercato digitale è rappresentato dall'attività svolta dalla Commissione circa l'applicazione del DMA.

Si tratta di un'applicazione rappresentata dalle sanzioni inflitte dalla Commissione a *Apple* (500 milioni di euro) e *Meta* (200 milioni di euro; *Meta Platform* è la società madre di *Facebook*, *Instagram*, *WhatsApp*). La Commissione aveva condotto un'indagine in virtù dell'art. 20 DMA (apertura del procedimento) e aveva applicato sanzioni, cioè ammende, in virtù degli articoli 29 (procedura di adozione di una decisione sull'inosservanza) e 30 DMA (irrogazione di un'ammenda), ritenendo violati gli articoli 5, 6, 7 sugli obblighi del *gatekeeper*.

Quanto ad *Apple*, il comportamento illecito consisteva nell'aver imposto agli sviluppatori di *app* (professionisti che creano applicazioni *software* per dispositivi come *smartphone* e *tablet*) di informare gli utenti circa l'esistenza di offerte alternative, più vantaggiose al di fuori *dell'App Store* (negozio digitale in cui gli utenti possono trovare, scaricare e acquistare applicazioni-app per i propri dispositivi mobili). Gli sviluppatori di *app* che distribuiscono le loro *app* tramite l'*App Store* di Apple dovrebbero invece essere in grado di fornire gratuitamente tali informazioni. *Apple* ha così violato l'obbligo di *anti steering*, cioè di "non indirizzamento": obbligo che impone ai *gatekeepers* (le grandi piattaforme tecnologiche come *Apple*, nonché *Meta*), di consentire agli utenti di trovare e utilizzare servizi esterni, concorrenti o alternativi, consentendo quindi di effettuare liberamente acquisti (senza passare per l'*App Store*). Insomma, è necessario informare e garantire gli utenti circa le alternative possibili per quanto riguarda la conclusione di contratti e la promozione di offerte senza imporre costi.

Apple, in questa vicenda, non ha dimostrato che le restrizioni sono oggettivamente necessarie e proporzionate; la Commissione, oltre alla sanzione, ha ordinato ad *Apple* di rimuovere le restrizioni tecniche e commerciali e di astenersi da un comportamento futuro non conforme alla decisione adottata.

Quanto a *Meta*, è stato ritenuto contrastante l'aver introdotto un modello o schema pubblicitario *Consent* or *Pay*, cioè offrire all'utente (di *Facebook* o *Instagram*) la scelta se accettare il tracciamento dei propri dati

per fini pubblicitari ("pubblicità personalizzata") oppure il pagamento di un abbonamento mensile per utilizzare la piattaforma senza pubblicità dei dati (la pubblicità sarebbe stata, quindi, disabilitata). La Commissione ha ritenuto che non fosse garantito un consenso libero, specifico e informato e non fosse offerta un'alternativa che facesse minor uso dei dati personali (meno personalizzata, dunque), ma equivalente al servizio di "pubblicità personalizzata". Il modello adottato non può avere effetti distorsivi sul mercato della pubblicità *online* perché al consumatore-utente devono essere offerte possibilità di scelta (la gratuità era subordinata ad accettazione della profilazione per finalità pubblicitarie; l'opzione pagamento veniva ritenuta una pressione economica).

Le due società hanno reagito contestando il diverso trattamento della Commissione a favore di imprese cinesi ed europee, e quindi la previsione di *standard* diversi, sottolineando come i limiti posti alla pubblicità personalizzata provocassero (e provochino) danni rilevanti. Le due società hanno presentato ricorso al Tribunale[19]: si vedrà il seguito.

[19] Cfr. cause T-435/25, *Meta Platforms c. Commissione* e T-438/25, *Apple c. Commissione*.

La tutela dell'impresa nel Mercato Unico Digitale

di VITTORIO BACHELET*

SOMMARIO: 1. *Data Act* e tutela dell'impresa. – 2. *Data Act*, DMA e i "dati" quali risorse economiche. – 3. Cenni al dibattito sull'ammissibilità dello scambio di dati personali contro servizi nel diritto europeo. – 4. *Data Act* e nuove frontiere degli scambi di dati. – 5. *Data Act* e tutela dell'impresa contro le clausole abusive. – 5.1. Ambito di applicazione: contratti e clausole. – 5.2. Il presupposto: l'imposizione unilaterale della clausola. – 5.3. Definizione generale di clausola abusiva. – 6. Considerazioni finali: il ruolo delle «clausole contrattuali tipo» nel *Data Act*.

1. *Data Act* e tutela dell'impresa

Discorrere di tutela dell'impresa nel Mercato Unico Digitale significa anzitutto esaminare la disciplina introdotta dal cosiddetto *Data Act*, ossia il Regolamento (UE) 2023/2854, recante norme armonizzate sull'accesso equo i dati e sul loro utilizzo, applicabile dal 12 settembre 2025[1]. Come si vedrà, infatti, il capo IV dedicato alle «clausole contrattuali abusive relative all'accesso ai dati e al relativo utilizzo tra imprese» comprende l'art. 13 che riguarda, in particolare, la protezione dell'impresa contro «clausole contrattuali abusive imposte unilateralmente da un'altra impresa».

Va segnalato fin da subito che tale disciplina presenta una significativa rilevanza sistematica: introduce, infatti, per la prima volta una regolamentazione europea delle clausole abusive nei contratti tra imprese[2]. In precedenza, si occupavano di squilibrio negoziale nei rapporti *business-to-business* soltanto le Direttive 2000/35/CE e 2011/7/EU relative alla lotta contro i ritardi di pagamento nelle transazioni commerciali[3]. Come noto,

* Professore associato di diritto privato presso l'Università Cattolica del Sacro Cuore, Milano.

[1] Su cui v., tra gli altri, V. BACHELET, G. MARINO, A. RACANO, (a cura di) *Data Act. Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi dell'orizzonte del diritto privato*, Milano, 2025, *passim*.

[2] Non essendosi mai tradotta in legge la «Proposta di Regolamento relativo a un diritto comune europeo della vendita», c.d. *Common European Sales Law* (CESL), adottata l'11 ottobre 2011, COM(2011) final.

[3] Cfr. la dir. 2000/35/CE, attuata nell'ordinamento italiano dal d.lgs. 9 ottobre 2002, n. 231, e poi trasfusa, con modificazioni, nella dir. 2011/7/UE, attuata dal d.lgs. 9 novembre 2012, n. 192.

assumendo il creditore quale parte debole del rapporto, esse qualificano come inefficaci, in particolare, le clausole gravemente inique relative al termine di pagamento, al saggio degli interessi moratori e al risarcimento dei costi di recupero[4].

Per il resto[5], la disciplina dello squilibrio nei contratti tra imprese restava tradizionalmente relegata al rango di eccezione nel diritto europeo della concorrenza, comportando norme più rigorose contro gli abusi unilaterali rispetto al divieto di abuso di posizione dominante, come le discipline nazionali in materia di abuso di dipendenza economica[6]. Nitida si rivela, allora, la portata sistematica di un regolamento che introduce un'articolata disciplina, immediatamente applicabile in tutti gli Stati membri, volta a sanzionare la stipulazione di clausole abusive nei contratti fra imprese.

Prima di illustrare tale innovativa disciplina, largamente ispirata a quella di cui alla Direttiva 93/13/CEE in tema di clausole abusive nel contratto del consumatore, è opportuno introdurre il *Data Act*: un regolamento ancora poco esplorato dalla dottrina italiana, a differenza di quella tedesca, e nondimeno di grande rilievo sia sotto il profilo teorico che applicativo.

2. *Data Act,* DMA e i "dati" quali risorse economiche

Come è noto, uno degli obiettivi centrali della "strategia europea dei dati" è contrastare la concentrazione del cosiddetto capitale informativo nelle mani di poche grandi piattaforme digitali[7]. Tale accumulazione rischia, infatti, di trasformarsi in un limite strutturale a uno sfruttamento più generalizzato e capillare dei dati, ormai intesi non più soltanto come

[4] Art. 7, par. 1, dir. 2011/7: clausole che, come è noto, sono qualificate in termini di nullità dall'art. 7, par. 1, d.lgs. 231/2002.

[5] Anche la più recente dir. 2019/633/EU in materia di pratiche commerciali sleali nei rapporti tra imprese nella filiera agroalimentare vieta, invero, talune clausole ingiustificatamente gravose, ma soltanto qualora non concordate in termini chiari e univoci: senza, dunque, sindacare il loro squilibrio intrinseco: cfr. l'art. 3, par. 2, recepito nell'art. 4, par. 4, d.lgs. 8 novembre 2021, n. 198.

[6] Art. 3, par. 2, e considerando n. 8 del Reg. 1/2003/CE concernente l'applicazione delle regole di concorrenza di cui agli artt. 101 e 102 TFUE.

[7] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni – Strategia europea dei dati*, COM(2020) 66 final, 19 febbraio 2020, p. 9. Per uno sguardo d'insieme, si veda G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, p. 971 ss.

"nuovo petrolio"[8], ma come una risorsa ancora più peculiare: un bene inconsumabile e non rivale, dotato di potenzialità inesauribili[9].

La risposta normativa dell'Unione si articola su più piani. A monte, il *Digital Markets Act* (DMA)[10] mira a garantire mercati digitali equi e contendibili attraverso una regolazione *ex ante* dei comportamenti delle maggiori piattaforme che assumono lo status di *gatekeeper* (lett. "controllori all'accesso")[11], recependo e sistematizzando principi già affermatisi nel diritto europeo e nazionale della concorrenza[12]. A valle, il *Data Act* si concentra sulla circolazione dei dati generati da prodotti connessi e servizi correlati nell'ambito del c.d. *Internet of Things*: non più ristretti alla dimensione "personale" tipica del GDPR[13], ma concepiti in senso lato come «qualsiasi rappresentazione digitale di atti, fatti o informazioni…», secondo la definizione già accolta dal *Data Governance Act* (DGA)[14].

Si passa così da una nozione di dato legata alla possibilità di identificare il soggetto di riferimento, l'interessato, a una nozione che guarda al dato – personale e insieme non personale – quale oggetto di valore, suscettibile di sfruttamento economico[15]. In questa prospettiva, i dati assumono, per l'appunto, la fisionomia di "capitale informativo": il *Data Act* ne promuove l'utilizzo e la condivisione, riconoscendo diritti di accesso in capo agli utenti dei prodotti connessi e dei servizi correlati, nonché obblighi di condivisione a favore di terzi – dai quali sono significativamente esclusi i *gatekeeper*[16] – (capo II e III)[17]; in talune

---

[8] Locuzione impiegata anche dal Commissario europeo per la tutela dei consumatori (M. Kuneva), *Discorso di apertura alla tavola rotonda* "*Online Data Collection, Targeting and Profiling*", Bruxelles, 31 marzo 2009, e, più di recente, dallo stesso Parlamento europeo, *Think tank*, *Is Data the New Oil? Competition Issues in the Digital Economy*, 8 gennaio 2020, *www.europarl.europa.eu/thinktank*.

[9] *Amplius*, V. BACHELET, *Il consenso oltre il consenso: dati personali, contratto, mercato*, Pisa, 2023, p. 33 s.

[10] Regolamento (UE) 2022/1925 del 14 settembre 2022.

[11] Cfr. l'articolata definizione di cui all'art. 3, par. 1, DMA.

[12] K. BANIA, *Fitting the Digital Markets Act in the Existing Legal Framework: The Myth of the "Without Prejudice" Clause*, in *Eur. Comp. J.*, 2023, p. 140.

[13] Secondo la nota definizione dell'art. 4, n. 1, del Regolamento (UE) 2016/679, per cui si considera dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile…».

[14] Regolamento (UE) 2022/868 del 30 maggio 2022 (art. 2, n. 1).

[15] Sul punto, per tutti, A. LAS CASAS, *Il Data Act nello scenario del capitalismo dell'informazione: dai "dati personali" ai "dati"*, in *Data Act*, cit., p. 14 ss., e già G. RESTA, *Pubblico, privato, collettivo*, cit., spec. p. 975.

[16] Art. 5, par. 3, e art. 6, par. 2, lett. *d*), *Data Act*.

[17] Vedi il successivo § 4.

ipotesi, anche a favore di enti pubblici (capo V)[18]. Proprio perché considera i dati quali beni dotati di valore economico, la disciplina interviene anche sul piano contrattuale introducendo strumenti di protezione non solo, come anticipato, contro la pattuizione di clausole abusive (capo IV), ma pure contro i fenomeni di cosiddetto *lock-in* nei servizi *cloud* (capo VI)[19], al fine di garantire che il patrimonio informativo incorporato nei dati non resti concentrato presso pochi "colossi digitali" e possa, al contempo, circolare senza che le asimmetrie tipiche dei mercati digitali ne ostacolino l'effettivo sfruttamento[20].

Il passaggio è significativo: se il GDPR ha disciplinato i dati in funzione della tutela dei diritti fondamentali della persona[21], il *Data Act* inaugura un sia pur embrionale statuto patrimoniale dei dati, volto a redistribuire ricchezza e "potere informazionale", proiettando strumenti privatistici al servizio di finalità di *policy* pubblica. Queste finalità riflettono l'impronta ordoliberale del modello europeo, che mira a rendere il mercato più efficiente[22]: non attraverso una mera *deregulation* in senso liberistico, bensì tramite regole volte a correggere le asimmetrie contrattuali[23]. In questa logica, il ruolo dello Stato come guida del processo economico lascia spazio a un incisivo intervento del diritto privato regolatorio[24], che limita l'autonomia privata a beneficio della concorrenza, della trasparenza e della correttezza degli scambi[25] (considerando 2, 4 e 5 del *Data Act*).

---

[18] Inclusa la Commissione, la Banca centrale europea e gli organismi dell'Unione: v., sul punto, E. CREMONA, *Obbligo di mettere a disposizione i dati sulla base di necessità eccezionali*, in *Data Act*, cit., p. 261 ss.

[19] Cfr. A. POTINI, *Passaggio tra servizi di trattamento dei dati. Obblighi tecnici e contrattuali*, in *Data Act*, cit., p. 297 ss., nonché S. IACONELLI, *I servizi di trattamento dei dati: perimetro della definizione*, ivi, spec. p. 290 ss.

[20] V. anche M. SCIALDONE, *Introduzione e obiettivi del Data Act*, in L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), *Data Act. Regolamento europeo sui dati*, Milano, 2025, spec. p. 2 s.

[21] Oltre che della libera circolazione dei dati personali: v. i paragrafi successivi.

[22] Lo ricorda E. NAVARRETTA, *Il contratto «democratico» e la giustizia contrattuale*, in *Riv. dir. civ.*, 2016, p. 1274 s. Sulla Scuola ordoliberale di Friburgo, v. G. AMATO, *Antitrust and the Bounds of Power*, Hart, Oxford, 1997, spec. p. 40 ss.

[23] V., per tutti, L. MENGONI, *Autonomia privata e Costituzione*, in *Banca borsa tit. cred.*, 1997, I, pp. 3 e 20.

[24] Cfr. A. ZOPPINI, *Il diritto privato e i suoi confini*, Bologna, 2020, pp. 188 ss. e 244 s.

[25] V. ancora, in generale, L. MENGONI, *op. cit.*, p. 20, e, con riguardo al *Data Act*, M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, in S. LOHSSE, R. SCHULZE e D. STAUDENMAYER (a cura di), *Private Law and the Data Act. Münster Colloquia on EU Law and the Digital Economy VIII*, Baden-Baden, 2024, p. 149 ss.

3. Cenni al dibattito sull'ammissibilità dello scambio di dati personali contro servizi nel diritto europeo

La delineata evoluzione del dato, considerato ormai alla stregua di una risorsa economica piuttosto che come latore di informazioni personali, risente del dibattito che ha accompagnato, a partire dal 25 maggio 2018, l'applicazione del GDPR. Esso ha, infatti, innescato un intenso dibattito sulla legittimità della pratica di offrire i propri dati per accedere "gratuitamente"[26] a taluni servizi, come i *social network*, i quali vengono remunerati dagli inserzionisti che pagano le piattaforme per ottenere spazi pubblicitari personalizzati sulle preferenze degli utenti.

La questione si pone perché il regolamento generale sulla protezione dei dati personali non prende posizione su questa pratica, pur diffusa, lasciando all'interprete il delicato compito di ricostruire la relativa regola in chiava sistematica. In proposito, il regolamento si limita, infatti, a stabilire che il consenso dell'interessato deve essere libero (art. 4, n. 11, GDPR), e che tale libertà va valutata tenendo nella «massima considerazione» l'eventualità che l'esecuzione di un contratto – inclusa la prestazione di un servizio – sia condizionata al suo rilascio (art. 7, par. 4, GDPR).

Quanto alla legittimità dello scambio di dati personali contro servizi, appare significativo che il diritto secondario dell'Unione, contrariamente ad alcuni auspici[27], non vieta tale pratica, astenendosi dal considerare il relativo consenso al trattamento automaticamente privo del requisito di libertà[28]; scelta normativa coerente, peraltro, con il fatto che il regolamento non mira soltanto, come già anticipato, a tutelare le persone fisiche in relazione al trattamento dei dati personali, ma altresì ad agevolare la libera circolazione di tali dati (art. 1, par. 1, GDPR)[29].

---

[26] Nonché di pubblicizzarli come tali: significativo, in tal senso, che AGCM, provv. 29 novembre 2018, n. 27432, in *Boll. Agcm*, n. 46/2018 (conf. TAR Lazio, Roma, 10 gennaio 2020, n. 260, e Cons. Stato 29 marzo 2021, n. 2631), abbia considerato ingannevole la pratica commerciale di *Facebook* consistente nel pubblicizzare il proprio servizio come gratuito (v., tra gli altri, A VIGORITO, *La "patrimonializzazione" dei dati personali a partire dalla recente controversia AGCM-Facebook*, in *Giustiziacivile.com*, 20 aprile 2020).

[27] Cfr. LIBE, *Draft report on the proposal for a General Data Protection Regulation*, 21 novembre 2013, 2012/0011(COD), Amd. n. 82.

[28] *Amplius*, V. BACHELET, *Il contratto di scambio di "servizi contro dati" (o contro prezzo)*, in *Riv. dir. civ.*, 2024, p. 1133 s.

[29] L'art. 1, par. 3, GDPR sembra, anzi, voler mettere in guardia dal far prevalere sistematicamente le istanze personalistiche sull'esigenza economica di circolazione dei dati, contrastando una tendenza tradizionale sovente riscontrabile tra le autorità di

D'altra parte, il diritto alla protezione dei dati riconosciuto dall'art. 8 della Carta di Nizza e della CEDU, al pari di ogni altro diritto fondamentale, non gode di una tutela assoluta, ma deve essere bilanciato con gli altri diritti fondamentali alla luce del principio di proporzionalità sancito dall'art. 52 della Carta[30]. Tra questi, come ricorda lo stesso considerando 4 del GDPR, vi è anche la libertà d'impresa[31], che risulterebbe eccessivamente sacrificata se lo scambio dati-servizi, praticato da molte piattaforme, fosse vietato in radice.

Certo, sebbene una lettura sistematica del diritto primario e secondario dell'Unione escluda l'automatica invalidità del consenso "remunerato" al trattamento, il controllo sulla sua integrità si mostra più rigoroso rispetto a quello operante in ambito contrattuale. Non basta, infatti, l'assenza dei vizi della volontà di cui all'art. 1427 c.c.: il consenso deve costituire esercizio effettivo dell'autodeterminazione informativa (*informationelle Selbstbestimmung*)[32], per cui esso non risulta libero se è prestato per accedere a servizi inaccessibili senza acconsentire al trattamento dei dati (ad esempio, *newsletter* contenenti informazioni non altrimenti reperibili a pagamento) e, al contempo, irrinunciabile senza gravoso sacrificio per l'utente, trattandosi di servizi "essenziali", come quelli sanitari o bancari[33].

Atteso il loro ruolo ormai insostituibile per ricevere informazioni e mantenere contatti sociali e professionali, lo stesso Comitato europeo per la protezione dei dati ha riconosciuto il carattere essenziale dei servizi di *social network*[34]. Su questa linea, la Corte di giustizia nel caso *Meta Platforms* ha, da un lato, escluso che il consenso reso per accedere a un

protezione dei dati: cfr. V. RICCIUTO, *L'equivoco della privacy*, Napoli, 88 e 114 ss.; F. PIZZETTI, *L'Autorità Garante tra protezione e libera circolazione dei dati personali, completamento del* Single Digital Market *e Intelligenza Artificiale*, in F. PIZZETTI (a cura di) *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021, p. 170. In generale, si rinvia a O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, 2015, p. 46 ss.

[30] V., in generale, I. ANRÒ, B. NASCIMBENE, *La tutela dei diritti fondamentali nella giurisprudenza della Corte di Giustizia: nuove sfide, nuove prospettive*, in *Riv. it. dir. pubbl. com.*, 2017, p. 323 ss.

[31] Che comprende anche il diritto di trattare i dati: v. le conclusioni dell'AG Jääskinen, 25 giugno 2013, C-131/12, *Google Spain*, § 95.

[32] V., ad es. T. RIHEM, *Freie Widerrufbarkeit der Einwilligung und Struktur der Obligation. Daten als Gegenleistung?*, in T. PERTOT (a cura di), *Rechte an Daten*, Tübingen, 2020, p. 181; conf. Cass. civ., 2 luglio 2018, n. 17278, in *Giur. it.*, 2019, p. 532.

[33] Cfr., per tutti, S. THOBANI, *Operazioni di tying e libertà del consenso*, in *Giur. it.*, 2019, p. 534 s., e la giurisprudenza citata alla nota precedente.

[34] EDPB, *Opinion 8/2024 on Valid Consent in the Context of Consent or Pay Models Implemented by Large Online Platforms*, 17 aprile 2024, § 86 ss.

servizio sia in sé viziato e ha, dall'altro, imposto a piattaforme social generaliste come *Facebook* e *Instagram* – prive di reali concorrenti che offrano servizi analoghi[35] senza trattamento dati – di fornire esse stesse agli utenti un'alternativa senza consenso al trattamento, se del caso a fronte di un ragionevole corrispettivo[36].

Tale arresto conferma che il diritto fondamentale alla protezione dei dati deve essere bilanciato con la libertà d'iniziativa economica delle imprese, le quali possono pertanto esigere dagli utenti un "prezzo" anziché il consenso a essere profilati e ricevere pubblicità mirata, purché di importo tale da consentire loro di scegliere liberamente tra "*pay*" e "*consent*". Vero è che, dopo l'introduzione di tale modello nel novembre 2023[37], la stragrande maggioranza degli utenti di *Meta* ha continuato a "pagare in dati": vuoi perché ignari dell'esistenza o della portata della nuova opzione, vuoi perché consapevolmente riluttanti a versare una somma mensile pur modesta (€12.99 per *Facebook* o *Instagram*, €7.99 dal novembre 2024)[38]. Non si può, tuttavia, desumere apoditticamente da tale dato empirico[39] che il prezzo per accedere alle piattaforme di *Meta* senza profilazione risulti in quanto tale irragionevole[40]. Il rischio è, altrimenti, quello di vanificare

---

[35] Essendo *LinkedIn* destinato a un'utenza professionale e *TikTok* a una specifica fascia di età, come evidenziano A.S. D'AMICO *et al.*, *Meta's Pay-or-Okay Model: An Analysis Under EU Data Protection, Consumer and Competition Law*, in *RENFORCE Working Paper*, 1/2024, p. 6.

[36] Corte giust., 4 luglio 2023, causa C-252/21, *Meta Platforms v. Bundeskartellamt*, ECLI: ECLI:EU:C:2023:537, spec. § 150, con nota di V. BACHELET, *La Corte di giustizia sul caso Meta: trattamento dei dati e "prezzo" del consenso*, in *Pactum*, 2023, p. 483 ss.

[37] La decisione di *Meta* di uniformarsi al *dictum* della Corte di giustizia è stata indotta dall'intervento, richiesto dal Garante norvegese, di EDPB, *Urgent Binding Decision 1/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)*, 27 ottobre 2023.

[38] Anche il prezzo per entrambi i servizi è stato ridotto (da €20.99 a €12.99) per venire incontro alle preoccupazioni della Commissione europea, che aveva avviato indagini sul modello "*pay-or-consent*" di *Meta* il 25 marzo 2024, constatando preliminarmente la violazione dell'art. 5, par. 2, DMA il 1° luglio 2024: v. *infra*.

[39] Che rispecchia il fenomeno del c.d. *free effect*, secondo cui il "prezzo zero" distorce le scelte degli utenti, che tendono a preferire servizi del tutto gratuiti anche se pagare una piccola somma migliorerebbe significativamente la protezione dei loro dati: cfr. OECD, *Quality Considerations in Digital Zero-Price Markets*, 2018, 35, e, in dottrina, K. SHAMPAN'ER, D. ARIELY, *How Small is Zero-price? The True Value of Free Products*, in *FRB of Boston Working Papers*, No. 6-16, 2006, spec. p. 12.

[40] Come sostenuto nel reclamo presentato al Garante austriaco da NOYB (*European Centre for Digital Rights*), 28 novembre 2023, §§ 40–53, consultabile all'indirizzo: *https://noyb.eu/sites/default/files/2023-11/Complaint%20-%20Meta%20Pay%20or%20Okay%20-%20REDACTED.pdf*; ma cfr. V. BACHELET, '*Pay-or-Consent' and Emerging Trends in Digital Contract Law*, in *ERPL*, 2024, p. 798 s.

l'equilibrato indirizzo della Corte di giustizia, escludendo che un qualsivoglia corrispettivo, fosse pure irrisorio, sia esigibile in luogo del consenso al trattamento.

Proprio su questa controversa linea si è posto, nondimeno, il Comitato europeo per la protezione dei dati in un parere sul modello *pay-or-consent*, secondo cui il consenso al trattamento risulta libero, ai sensi del GDPR, solo se le grandi piattaforme offrono una terza scelta – gratuita e senza trattamento dei dati – oltre al pagamento "in dati" e al pagamento in denaro[41]. Un tale esito appare insostenibile non solo sul piano giuridico, essendo in contrasto con il sistema normativo, ma anche sotto il profilo economico: in nome della massima protezione dei dati, si finirebbe infatti per rendere "fuori legge" *tout court* le più evolute forme di scambio dati-servizi, tanto diffuse quanto apprezzate per aver permesso lo sviluppo e la diffusione a costo zero di servizi avanzati, spesso diventati indispensabili nella vita quotidiana.

Certo, ciò non significa che il modello *pay-or-consent* sia privo di criticità: esso richiede, infatti, un adeguamento che consenta agli utenti una scelta realmente libera, superando l'alternativa secca tra un consenso prestato in blocco a tutti i trattamenti dei dati[42], per accedere gratuitamente al servizio, e il pagamento di una tariffa piena, rifiutando ogni trattamento. In questa prospettiva, la Commissione ha da ultimo rilevato che il modello *pay-or-consent* di *Meta* viola il DMA[43], poiché non offre una terza opzione – intermedia tra consenso e pagamento – che comporti meno trattamenti e una minore personalizzazione della pubblicità, garantendo comunque un servizio equivalente, per assicurare una scelta effettivamente libera[44].

Desta, tuttavia, perplessità che la gratuità sia stata considerata un aspetto essenziale di tale equivalenza, quando un più equilibrato bilanciamento dei diritti fondamentali avrebbe indicato piuttosto una

[41] EDPB, *Opinion 8/2024*, cit., § 180 s.

[42] Una scelta ponderata presuppone, infatti, *ex* art. 4, n. 11, GDPR un consenso libero e specifico, da esprimersi in modo "granulare" per ciascuna delle finalità del trattamento (considerando 32); se non è possibile esprimere un consenso separato a distinti trattamenti, nonostante sia appropriato nel singolo caso, esso si presume non libero (considerando 43). In dottrina, v. G. RESTA, V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. proc. civ.*, 2018, p. 434.

[43] In particolare, l'art. 5, par. 2, là dove consente a un *gatekeeper*, come *Meta*, di combinare i dati personali degli utenti ai sensi delle lett. *a-c*), soltanto se offre loro una scelta specifica in tal senso ed essi prestano un consenso valido a norma del GDPR: cfr. Sintesi della decisione della Commissione del 23 aprile 2025, *Case DMA.100055 – Meta – Article 5(2)*, C/2025/3466.

[44] Cfr. i considerando nn. 36 e 37 DMA.

"terza via" a tariffa ridotta, idonea a compensare i minori introiti dell'impresa derivanti dalla minore personalizzazione della pubblicità[45].

4. *Data Act* e nuove frontiere degli scambi di dati

Nel fare salva l'applicazione del GDPR[46], il *Data Act* risente del dibattito che ha condotto la stessa Corte di giustizia ad ammettere, sia pure a certe condizioni, lo scambio di dati personali contro servizi. In tal senso, si comprende perché esso faccia ormai riferimento, senza mezzi termini, ai «dati forniti in cambio» *ex* art. 13, par. 8, e concepisca, come anticipato, i dati (personali e non personali) alla stregua per l'appunto di una risorsa economica.

Il regolamento si concentra, in particolare, sui dati generati da attività di persone e macchine, nonché dalle loro interazioni, nell'ambito del c.d. *Internet of Things* (IoT)[47]. L'esigenza di disciplinare questo settore in rapida evoluzione è emersa dapprima nell'ordinamento tedesco, in particolare, nel dibattito sull'industria automobilistica connessa[48]. Si è così ravvisata la necessità di superare una situazione in cui lo sfruttamento economico del crescente volume di dati provenienti da prodotti connessi e servizi correlati[49] spettava, di fatto, ai produttori o fornitori, in virtù della loro posizione tecnica privilegiata di accesso. Come sottolineano i considerando iniziali, un obiettivo primario del *Data Act* è quello di riconoscere agli utenti diritti di accesso e di utilizzo, proprio per ovviare a tale "predominio di fatto"[50].

In tale logica, l'art. 4 del regolamento riconosce all'utente il diritto di ottenere dal titolare dei dati[51] l'accesso ai dati generati dall'uso del

---

[45] *Amplius*, V. BACHELET, '*Pay-or-Consent' and Emerging Trends in Digital Contract Law*, cit., 2024, p. 799 ss.

[46] Art. 1, par. 5, *Data Act*: cfr. M. SCHMIDT-KESSEL, *Einordnung des Data Act in das Mehrebenensystem des Unionsprivatrechts*, in *MMR*, 2024, p.127.

[47] V. l'art. 1, parr. 1-2, lett. *a*), e le note seguenti.

[48] Lo ricorda A. LAS CASAS, *Il Data Act nello scenario del capitalismo dell'informazione*, cit., p. 16.

[49] A proposito di tali definizioni di cui all'art. 2, nn. 5 e 6, si rinvia ad A. RACANO, *Prodotti connessi, servizi correlati e dati: definizioni e ambito oggettivo di applicazione del Capo II del Data Act*, in V. BACHELET, G. MARINO, A. RACANO, (a cura di), op. cit. p. 49 ss.

[50] Sul contenuto e sulla natura di tali diritti, v. *amplius* G. VERSACI, *I nuovi diritti ai sensi del Data Act: accesso ai dati, utilizzo e condivisione dei dati con terzi*, in *Data Act*, cit., p. 126 ss.

[51] Su tale definizione di cui all'art. 2, n. 13, v. criticamente C. ANGIOLINI, *Titolari dei dati, utenti, destinatari dei dati: ambito soggettivo di applicazione*, in V. BACHELET, G. MARINO, A. RACANO, (a cura di), op. cit., p. 89 ss., ma anche G. MARINO, *Questioni terminologiche, sovrapposizioni normative e applicazioni pratiche*, ivi, p. 110 ss.

prodotto connesso e del servizio correlato, insieme ai pertinenti metadati necessari a interpretarli e utilizzarli. Tale diritto, pur concepito in termini ampi, è temperato da alcune cautele: restano, infatti, esclusi i dati derivati o dedotti – per salvaguardare gli investimenti e il *know-how* del titolare dei dati[52], e possono essere pattiziamente previsti limiti ulteriori per esigenze di sicurezza, tutela della salute o protezione delle persone fisiche[53].

In questo quadro, il *Data Act* prefigura rapporti contrattuali tra utente e titolare dei dati (artt. 3 e 4), volti a disciplinare l'accesso ai dati generati dall'uso di prodotti connessi e servizi correlati. Tali rapporti possono instaurarsi tanto in contesti *business-to-consumer* quanto *business-to-business*[54]: si pensi, rispettivamente, al consumatore che eserciti il proprio diritto di accesso per analizzare autonomamente i dati del proprio *smartwatch*, o all'impresa agricola che ottenga i dati del proprio trattore intelligente per utilizzarli nella gestione delle colture e nella pianificazione della manutenzione, secondo le proprie necessità operative[55].

Parallelamente, l'art. 5 riconosce all'utente il diritto di chiedere al titolare la trasmissione diretta dei dati a terzi da lui designati, qualificati come destinatari dei dati[56]. In questo caso, il rapporto contrattuale si instaura tra il titolare dei dati e il destinatario, configurandosi in un contesto tipicamente *business-to-business*[57]. Tale disposizione è quella che apre chiaramente alla costruzione di un mercato regolato degli scambi di dati, in cui il titolare non può opporsi alla richiesta dell'utente, se non per comprovate ragioni di sicurezza o tutela della riservatezza, e deve rendere i dati disponibili a condizioni eque, ragionevoli e non discriminatorie, ai sensi dell'art. 8 del *Data Act*[58]. A titolo esemplificativo, si pensi a un

[52] Su tali profili, v. G. REMOTTI, *I nuovi diritti e la disciplina sui segreti commerciali*, in V. BACHELET, G. MARINO, A. RACANO, (a cura di) *op.* cit., p. 177 ss., e A. MICHINELLI, *Diritti e obblighi degli utenti e dei titolari dei dati*, in *Data Act. Regolamento*, cit., p. 97 ss.

[53] Art. 4, par. 2, *Data Act*.

[54] A. D'ADDAZIO, E. ROSSI, *Il Data Act e la redazione dei contratti*, in V. BACHELET, G. MARINO, A. RACANO, (a cura di) *op. cit*., p. 163 ss.

[55] Con riguardo ai contratti conclusi nel contesto dell'art. 4 Data Act, v., *amplius*, A. METZGER e H. SCHWEITZER, *Shaping Markets: A Critical Evaluation of the Draft Data Act*, in *ZEuP*, 2023, p. 62 ss.

[56] Cfr. G. VERSACI, *I nuovi diritti ai sensi del Data Act: accesso ai dati, utilizzo e condivisione dei dati con terzi*, cit., p. 136 ss., e A. MICHINELLI, *Diritti e obblighi degli utenti e dei titolari dei dati*, cit., p. 84 ss.

[57] A. D'ADDAZIO, E. ROSSI, *Il Data Act e la redazione dei contratti*, cit., p.168 ss.

[58] In tema di condizioni "*fair, resonable and non-discriminatory*" (c.d. FRAND) nel contesto del *Data Act*, v., ad es., G. FIORDALISI, *Obblighi per i titolari tenuti a mettere a*

produttore di macchinari industriali intelligenti che, su richiesta di un'impresa cliente, trasferisca i dati di funzionamento a una piattaforma specializzata nella gestione operativa e nella manutenzione predittiva[59].

In questa prospettiva, il *Data Act* favorisce l'emersione di nuove figure imprenditoriali – intermediari di dati, piattaforme di scambio, fornitori di servizi basati sui dati – capaci di generare valore economico senza detenere necessariamente il controllo materiale o tecnico del prodotto da cui i dati originano. Ne risulta una moltiplicazione delle possibili relazioni contrattuali attorno al dato: dal contratto tra utente e titolare, a quello tra titolare e destinatario, fino a scenari più complessi che coinvolgono una pluralità di utilizzatori[60]; con l'obiettivo, per l'appunto, di sottrarre al produttore o al fornitore la posizione di monopolio di fatto per restituire all'utente la possibilità di decidere come sfruttare i dati generati dall'uso del prodotto o del servizio.

5. *Data Act* e tutela dell'impresa contro le clausole abusive

Il *Data Act* promuove, dunque, l'utilizzo e la condivisione dei dati, quali beni dotati di valore economico, nella prospettiva del diritto privato regolatorio. A tal fine, da un lato, individua con chiarezza diritti di accesso e di utilizzo dei dati in capo agli utenti dei dispositivi connessi e dei servizi correlati, siano essi consumatori o imprese; dall'altro, contrasta gli squilibri contrattuali che altrimenti ostacolerebbero il pieno sfruttamento e la circolazione negoziale dei dati, con l'obiettivo di favorirne un'allocazione più efficiente a vantaggio della collettività (considerando 2, 4 e 5)[61].

In questo senso, si coglie l'importanza di una disciplina privatistica volta a tutelare l'impresa contro la stipulazione di clausole contrattuali abusive[62]. A differenza del consumatore, che resta protetto in generale

---

disposizione i dati a norma del diritto dell'Unione, in *Data Act. Regolamento*, cit., p. 129 s., 136 ss., e S. LOUVEN, *Vorschriften im Data Act zur Ausgestaltung und Kompensation von Datenbereitstellungspflichten*, in *MMR*, 2024, p. 82 ss.

[59] Con riguardo ai contratti conclusi nel contesto dell'art. 5 *Data Act*, cfr. A. METZGER e H. SCHWEITZER, *Shaping Markets*, cit., p. 64 s.

[60] V., ancora, A. D'ADDAZIO, E. ROSSI, *Il Data Act e la redazione dei contratti*, cit., p. 168.

[61] Insiste sul punto anche G. VERSACI, *I nuovi diritti ai sensi del Data Act: accesso ai dati, utilizzo e condivisione dei dati con terzi*, cit., p. 125 ss.

[62] A proposito della quale, si rinvia a V. BACHELET, *Clausole abusive unilateralmente imposte nei contratti tra imprese*, in V. BACHELET, G. MARINO, A. RACANO, (a cura di), op. cit., p. 219 ss.; v. anche M. SCIALDONE, *Le clausole abusive per l'accesso ai dati*, in *Data act. Regolamento*, cit., p. 163 ss.

dalla Direttiva 93/13/CEE[63] – applicabile, ad esempio, al contratto fra titolare dei dati e utente (consumatore) di prodotti connessi o servizi correlati[64] – l'impresa non godeva in precedenza di una tutela contro le clausole squilibrate, se non nei limitati termini segnalati all'inizio.

Proprio sulla Direttiva 93/13 si modella, come anticipato, l'innovativa disciplina delle clausole abusive nei contratti tra imprese di cui all'art. 13 del *Data Act*[65].

5.1. Ambito di applicazione: contratti e clausole

Pur non avendo portata generale, a differenza della Direttiva 93/13 nei rapporti tra professionista e consumatore, la disciplina di cui all'art. 13 del *Data Act* presenta un ambito di applicazione ampio[66], riferendosi a tutti i contratti tra imprese private concernenti l'accesso e l'utilizzo di dati[67], con esclusione di quelli stipulati con enti pubblici o non profit.

In tale nozione, rientrano anzitutto i contratti già menzionati conclusi fra titolare dei dati e utente in materia di accesso, utilizzo o messa a disposizione dei dati generati dal prodotto connesso o dal servizio correlato (art. 4), nonché i contratti stipulati fra titolare dei dati e terzi per la messa a disposizione dei dati (art. 5)[68]. Nell'ampia definizione di contratti su cui si basa l'accesso o l'utilizzo di dati rientrano, peraltro, anche contratti diversi[69], come quelli per la messa a disposizione dei dati conclusi dall'utente direttamente con un terzo, senza coinvolgimento del titolare dei dati, o quelli conclusi dal titolare dei dati con un terzo, senza che vi sia stata una specifica richiesta dell'utente.

In generale, la disciplina si applica a tutti i contratti nell'ambito dei quali le parti trasmettono dati, purché tale trasferimento costituisca – se non l'oggetto principale – almeno una prestazione accessoria autonoma, negoziata separatamente o tale da incidere sulla determinazione del corrispettivo complessivo[70]. In tal senso, essa si estende anche ai contratti

---

[63] La cui applicazione è fatta salva dall'art. 1, par. 9, del *Data Act.*

[64] V. il considerando 28 del *Data Act.*

[65] Lo rileva, tra gli altri, S. SCHWAMBERGER, *Die Klauselkontrolle in Art. 13 Data Act*, in *MMR-Beil*, 2024, p. 98.

[66] Cfr., ad es., M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, in S. LOHSSE, R. SCHULZE e D. STAUDENMAYER (a cura di), cit., p. 156.

[67] Art. 1(2), lett. *c*), *Data Act*.

[68] S. OMLOR, *Unfair Contractual Terms under the EU Data Act*, in *ERPL*, 2024, p. 179.

[69] Lo segnala anche D. STAUDENMAYER, *Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz*, in *EuZW*, 2022, p. 596 s.

[70] Cfr. M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, in S. LOHSSE, R. SCHULZE e D. STAUDENMAYER (a cura di), cit., p. 157.

di vendita di dispositivi IoT, inclusi quelli riguardanti immobili "intelligenti", escludendo invece le comuni vendite in cui il venditore è semplicemente tenuto a fornire all'acquirente dati relativi all'immobile compravenduto. Il *Data Act* tratta infatti i dati alla stregua di una risorsa economica, sicché rimangono ad esso estranei soltanto i contratti rispetto ai quali i dati risultano meramente accessori[71].

Si tratta di contratti verosimilmente destinati a moltiplicarsi con l'applicazione del *Data Act*, che regola la circolazione dei dati proprio al fine di promuovere lo sviluppo di un mercato dalle rilevanti potenzialità di crescita. In questa prospettiva, l'art. 13, par. 1, sottopone al controllo di abusività, in particolare, le clausole contrattuali concernenti l'accesso ai dati e il relativo utilizzo, nonché la responsabilità e i mezzi di ricorso per la violazione o la cessazione degli obblighi relativi ai dati. Restano, invece, escluse le parti del contratto non correlate alla messa a disposizione dei dati[72].

Tuttavia, l'estensione di tale controllo alle clausole che, pur non riguardando direttamente l'accesso e l'utilizzo dei dati, disciplinano la responsabilità e i rimedi in caso di violazione o di cessazione degli obblighi relativi ai dati conferisce alla disciplina una portata decisamente ampia[73]. Non sorprende, dunque, se molte clausole qualificabili come abusive rinviano a profili generali di squilibrio contrattuale, che trascendono il contesto specifico dell'accesso e dell'utilizzo dei dati: basti pensare alle clausole volte a escludere la responsabilità dell'impresa che ha imposto unilateralmente la pattuizione, ovvero che, in caso di inadempimento della stessa, escludono i mezzi di ricorso a disposizione della controparte[74].

Da ciò discende che la disciplina in esame non ha una portata meramente settoriale, ma presenta rilevanza generale nell'ambito del diritto dei contratti.

---

[71] V. la nt. precedente. A titolo esemplificativo, l'art. 13 del *Data Act* si estende ai contratti di condivisione di dati nel settore dell'Intelligenza Artificiale (IA), ad esempio, tra imprese che cedono dati relativi a operazioni industriali e commerciali, o a cartelle cliniche anonimizzate, per addestrare modelli di *machine learning* e sviluppare algoritmi predittivi e soluzioni automatizzate: per una più ricca esemplificazione, cfr. V. BACHELET, *Clausole abusive unilateralmente imposte nei contratti tra imprese*, cit., p. 222 s.

[72] Considerando 60 *Data Act*.

[73] Lo nota, ad esempio, S. SCHWAMBERGER, *Die Klauselkontrolle in Art. 13 Data Act*, cit., p. 98.

[74] Art. 13, par. 3, lett. *a*-*b*), *Data Act*.

5.2. Il presupposto: l'imposizione unilaterale della clausola

L'art. 13 del *Data Act* non individua a priori categorie di imprese meritevoli di tutela contro la pattuizione di clausole abusive. A differenza delle discipline che proteggono il consumatore in quanto parte strutturalmente debole del rapporto con il professionista[75], richiede un accertamento concreto, ed *ex post*, della posizione di debolezza dell'impresa. Tale approccio è proprio delle normative che non proteggono imprese tipicamente deboli in certe categorie di relazioni commerciali (come la subfornitrice o l'affiliata nel *franchising*)[76], ma qualsiasi impresa che, nel singolo rapporto, si trovi in una situazione di effettiva debolezza rispetto alla controparte, come ad esempio l'impresa economicamente dipendente[77].

A tale proposito, la disciplina in esame esige che la clausola abusiva sia stata imposta unilateralmente all'impresa che invoca tutela (art. 13, par. 1), vale a dire quando la controparte non sia stata in grado di influenzarne il contenuto, malgrado il tentativo di negoziarla (art. 13, par. 6), trovandosi perciò costretta a "prendere o lasciare" (considerando 59). Richiedendo una condotta attiva dell'impresa che invoca tutela, consistente nel tentativo infruttuoso di negoziazione, la disciplina pone un presupposto più stringente rispetto a quello previsto per i contratti dei consumatori dalla Direttiva 93/13, che considera sufficiente la mancata negoziazione individuale della clausola predisposta dal professionista (art. 3, par. 2)[78].

L'onere di dimostrare che la clausola sia stata imposta unilateralmente non grava, tuttavia, sull'impresa protetta, spettando invece all'impresa che l'ha inserita nel contratto provare di non averla imposta (art. 13, par. 6, *Data Act*). In virtù di tale inversione probatoria, il rigore sostanziale del presupposto del controllo di abusività si attenua sul piano processuale[79],

---

[75] V., per tutti, S. MAZZAMUTO, *Il contratto di diritto europeo*, Torino, 2017, p. 172.

[76] Ai sensi, rispettivamente, della Legge 192/1998 e della Legge 129/2004.

[77] Sul tema, si rinvia a V. BACHELET, *Abuso di dipendenza economica e squilibrio nei contratti tra imprese*, Milano, 2020, spec. p. 231 ss.; per una panoramica su altre discipline nazionali dell'abuso di dipendenza economica, v. ID., *The Abuse of Economic Dependence "Digitalization": The Italian Novella in Context*, in *Eur. Comp. Law Rev.*, 2023, p. 301.

[78] Cfr. S. OMLOR, *Unfair Contractual Terms*, cit., pp. 177 s. e 180; A. WIEBE, *Der Data Act als vertragsrechtlicher Rahmen für Datennutzungsverträge. Anwendungsbereich und Vorgaben der Missbrauchskontrolle nach Art. 13 Data Act-E*, in *CR*, 2023, p. 789. Viceversa, l'assenza di una trattativa individuale costituisce il presupposto per il giudizio sull'abusività delle clausole tanto nei contratti dei consumatori, quanto nei contratti tra imprese, nell'ambito dei *Principles of European Contract Law* (PECL, art. 4:110) e i Principi *Acquis* (art. 6:301-2).

[79] V. anche A. WIEBE, *Der Data Act als vertragsrechtlicher*, cit., p. 780.

essendo sufficiente per l'impresa allegare che la clausola le sia stata imposta unilateralmente, senza doverne fornire la dimostrazione[80].

In tale prospettiva, la norma introduce un notevole incentivo a una effettiva negoziazione tra le parti[81]: per fornire la prova contraria, l'impresa predisponente dovrà, infatti, dimostrare che l'oblata ha omesso il tentativo di negoziazione, ovvero che è riuscita a influenzare il contenuto della clausola contestata[82] (ad esempio, tramite l'esibizione degli scambi via-email tra le parti)[83]. E se certo l'accettazione senza obiezioni è idonea a sottrarre la clausola al controllo di abusività[84], anche un tentativo meramente formale di trattativa – verosimilmente destinato a fallire in un rapporto, per l'appunto, asimmetrico – va ritenuto sufficiente ai fini dell'applicabilità della disciplina in esame, in modo da salvaguardarne le finalità protettive dell'impresa debole.

Atteso il forte incentivo per le imprese a documentare un siffatto tentativo e le difficoltà del predisponente nel dimostrare il contrario, a quest'ultimo spesso resterà provare, per salvaguardare le clausole, che l'aderente ne abbia effettivamente influenzato il contenuto. In tal senso, il *Data Act* non mira solo a sanzionare la pattuizione di clausole abusive riguardanti l'accesso e l'utilizzo dei dati, nonché la responsabilità e i rimedi in caso di violazione o cessazione dei relativi obblighi, ma anche a promuovere prassi contrattuali più equilibrate, scoraggiando l'uso di clausole predisposte e non negoziate.

5.3. Definizione generale di clausola abusiva

L'art. 13, par. 3, del *Data Act* qualifica in generale come abusiva la clausola «di natura tale che il suo utilizzo si discosta considerevolmente dalle buone prassi commerciali in materia di accesso ai dati e relativo utilizzo, in contrasto con il principio di buona fede e correttezza». Nella prospettiva del civilista, tale definizione richiama quella di clausola abusiva della Direttiva 93/13, incentrata sul significativo squilibrio dei

[80] Cfr. C. GALLESE, *A First Commentary to the Proposal for a new Regulation on Fair Access and Use of Data (Data Act)*, in *Medialaws*, 2022, p. 268.
[81] Lo evidenziano, tra gli altri, M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, cit., p. 158 s., e S. SCHWAMBERGER, *Die Klauselkontrolle in Art. 13 Data Act*, cit., p. 98.
[82] V. il considerando n. 59 del *Data Act*.
[83] D. STAUDENMAYER, *Der Verordnungsvorschlag*, cit., p. 601; cfr. A. WIEBE, *Der Data Act als vertragsrechtliche*, cit., p. 780,
[84] V. il considerando 59 del *Data Act*.

diritti e degli obblighi contrattuali a danno del consumatore, in contrasto con il requisito della buona fede.

Prima di soffermarsi sul rilievo della violazione della buona fede, comune alle due definizioni, occorre osservare che quella del *Data Act* si distingue per il riferimento al considerevole scostamento dalle buone prassi commerciali[85]. Ciò che emerge con chiarezza è l'intento di salvaguardare la libertà contrattuale tra imprese, colpendo soltanto le clausole «eccessive»[86], in linea con l'approccio ordoliberale che ispira la normativa.

Resta, tuttavia, il problema dell'indeterminatezza del parametro valutativo dell'abusività, destinato peraltro ad aggravarsi in un quadro normativo volto ad armonizzare il mercato interno[87], ancora privo di prassi consolidate di riferimento[88]. Le incertezze riguardano, in sintesi: cosa si intenda per «prassi commerciali», in particolare se si faccia riferimento a usi transnazionali o locali; cosa si intenda per «buone» prassi, e segnatamente se vadano valutate alla luce delle regole di deontologia professionale, o in base a criteri più generali che considerino anche altri interessi[89]; cosa si intenda per clausole il cui impiego «si discosta considerevolmente» dalle buone prassi commerciali[90], fra le quali il considerando 61 annovera, senza sciogliere i dubbi, la pratica di

---

[85] Analogamente a quanto già previsto, in materia di clausole abusive nei contratti tra professionisti, dal *Draft Common Frame of Reference* (DCFR, II. – 9:405) e dai Principi *Acquis* (art. 6:301-2); mentre i *Principles of European Contract Law* individuano nel significativo squilibrio nei diritti e nelle obbligazioni contrattuali un parametro applicabile non solo ai contratti dei consumatori, ma anche a quelli tra professionisti, senza menzionare lo scostamento – sostanziale o notevole – dalle buone prassi commerciali (PECL, art. 4:110).

[86] Considerando 59 e 61 del *Data Act*.

[87] Considerando 4 del *Data Act*.

[88] Cfr. M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, cit., p. 160.

[89] Solleva tali perplessità, in relazione all'omologo parametro valutativo dell'abusività delle clausole nei contratti tra professionisti *ex* art. 86(1) della proposta CESL, M. MAUGERI, *Il controllo sulle clausole abusive nei contratti fra imprese: dal modello delineato nei §§ 305 ss. del BGB a quello della CESL*, in *Nuova giur. civ. comm*., 2013, II, p. 117 ss. Analogamente, sottolineando l'assenza di usi commerciali riconosciuti a livello europeo, v. anche F.P. PATTI, *Le clausole abusive e l'*"optional instrument" *del percorso dell'armonizzazione in Europa*, in *Contr. impr./Eur.*, 2011, p. 683.

[90] Discorre delle buone pratiche commerciali e della "gross deviation" come di nozioni largamente oscure nell'ambito del *Data Act,* B. KARSTEN, *Unfair Terms for Data Access and Use between Enterprises (Art. 13)*, in, M. HENNEMANN, G.K. EBNER, B. KARSTEN, G. LIENEMANN, M. WIENROEDER (a cura di), *Data Act. An Introduction*, Nomos, Baden-Baden, 2024, p. 146.

pregiudicare oggettivamente la capacità della controparte di tutelare il suo legittimo interesse commerciale sui dati.

Quanto al rilievo della violazione della buona fede oggettiva, bisogna chiarire se essa rappresenti un requisito alternativo al grave scostamento dalle buone prassi commerciali (come suggeriscono le versioni tedesca[91] e polacca dell'art. 13, par. 3, *Data Act*), cumulativo[92] (in linea con le versioni croata, slovena e maltese dello stesso), ovvero – come indica la virgola impiegata nella maggior parte delle versioni linguistiche della disposizione (a partire da quelle francese e inglese, oltre che italiana) – un requisito non del tutto autonomo, implicito nell'imposizione di clausole che deviano considerevolmente dalle buone prassi commerciali[93].

In quest'ultima prospettiva, per attribuire alla violazione della buona fede un rilievo effettivo, seppur non autonomo, si possono ritenere scorrette non tutte le clausole che si discostano in maniera considerevole dalle buone prassi, ma solo quando lo scostamento appare ingiustificato alla luce delle circostanze di specie[94]. La violazione della buona fede opera così quale parametro integrativo del giudizio di abusività, garantendone l'aderenza al caso concreto[95], in linea con l'obiettivo del *Data Act* di sanzionare l'effettivo abuso di una posizione negoziale più forte[96].

Per garantire certezza, la definizione generale di clausola abusiva è affiancata da due elenchi di clausole considerate indicativamente abusive[97]: la lista "nera", che configura una presunzione assoluta di

---

[91] «Vertragsklauseln sind missbräuchlich, wenn ihre Anwendung eine grobe Abweichung von der guten Geschäftspraxis bei Datenzugang und Datennutzung darstellt oder gegen das Gebot von Treu und Glauben verstößt» (enfasi aggiunta).

[92] In tal senso, prendendo le distanze dalla versione tedesca del testo normativo, A. WIEBE, *Der Data Act als vertragsrechtliche*, cit., p. 782, testo e nt. 32.

[93] V., ad es., S. SCHWAMBERGER, *Die Klauselkontrolle in Art. 13 Data Act*, cit., p. 98.

[94] Così, con riguardo al «grave scostamento dalla prassi commerciale in contrasto con il principio di buona fede e correttezza», di cui all'art. 7, co. 2, d.lgs. 231/2002, modificato in attuazione dell'art. 7, co. 1, lett *a*), della dir. 2011/7 sui ritardi di pagamento nelle transazioni commerciali, A.M. BENEDETTI e M. GRONDONA, *La nullità delle clausole derogatorie nella nuova disciplina sui ritardi di pagamento*, in *Nuove leggi civ. comm.*, 2013, pp.1083 e 1088, testo e spec. nt. 22.

[95] È, del resto, questa l'interpretazione più convincente anche della definizione di clausola abusiva che, «in contrasto con il requisito della buona fede», determina un significativo squilibrio a danno del consumatore dei diritti e degli obblighi contrattuali. Ai sensi della Direttiva 93/13, la buona fede comporta, infatti, «una valutazione globale dei vari interessi in causa» (considerando 16), nell'ambito di un giudizio sull'abusività della clausola che tiene conto di tutte le circostanze della conclusione del contratto (art. 4, par. 1, dir.). Cfr., per ulteriori spunti e riferimenti, V. BACHELET, *Clausole abusive unilateralmente imposte nei contratti tra imprese*, cit., p. 235.

[96] Considerando 61 del *Data Act*.

[97] Considerando 62 del *Data Act.*

abusività (art. 13, par. 4), e la lista "grigia", che introduce una presunzione soltanto relativa (art. 13, par. 5)[98], combinando così i diversi gradi di certezza proprie delle due liste con la massima flessibilità della clausola generale[99]. Oltre alle liste di clausole indicativamente abusive, l'art. 13 del *Data Act* detta anche ulteriori norme in tema di salvaguardia delle clausole che riproducono disposizioni del diritto dell'Unione e di quelle che riguardano il profilo "economico" del contratto (parr. 2 e 8), nonché norme in merito alle conseguenze della valutazione di abusività (par. 7): profili per l'esame dei quali si rinvia a una trattazione dedicata[100].

6. Considerazioni finali: il ruolo delle «clausole contrattuali tipo» nel *Data Act*

La disciplina delle clausole abusive nei contratti *business-to-business*, di cui all'art. 13 del *Data Act*, ridefinisce i confini della tutela dell'impresa nel Mercato Unico Digitale. Come rilevato, essa si inserisce nell'ambito di un regolamento che considera i dati alla stregua di beni ormai dotati di valore economico, alla luce dell'evoluzione del dibattuto circa l'ammissibilità dello scambio di dati personali contro servizi ai sensi del GDPR.

In questo scenario, il regolamento in esame promuove l'uso e la condivisione dei dati: da un lato, riconoscendo diritti di accesso e di utilizzo in capo agli utenti dei dispositivi connessi e dei servizi correlati – siano essi consumatori o imprese; dall'altro, contrastando gli squilibri contrattuali che potrebbero ostacolare la circolazione dei dati e il loro pieno sfruttamento, favorendone un'allocazione più efficiente a vantaggio della collettività. Il *Data Act* non si limita, tuttavia, a introdurre strumenti innovativi di protezione dell'impresa, modellati sulla Direttiva 93/13/CEE, per sanzionare le clausole abusive unilateralmente imposte, ma si propone anche di promuovere pattuizioni più equilibrate, pur maturate in contesti negoziali asimmetrici.

---

[98] Oltre al considerando 62, secondo cui il *Data Act* «stabilisce un elenco di clausole che sono sempre reputate abusive e un elenco di clausole che si presumono abusive» (quest'ultima confutabile dall'impresa che ha imposto la clausola, dimostrando che essa «non è, nel caso di specie, abusiva»), rileva altresì l'uso della locuzione «è abusiva» nell'art. 13, par. 4, contrapposta alla locuzione «si presume» di cui all'art. 13, par. 5. In dottrina, v. ad es. M. HENNEMANN, *A Fair Share? Data Contracts and Unfair Terms Control*, cit., p. 167, e B. KARSTEN, *Unfair Terms for Data Access and Use between Enterprises (Art. 13),* cit., p. 145, ove ulteriori riferimenti.

[99] Cfr. D. STAUDENMAYER, *Der Verordnungsvorschlag*, cit., p. 598.

[100] V. BACHELET, *Clausole abusive unilateralmente imposte nei contratti tra imprese*, cit., p. 237 ss.

In questo senso, si segnala l'istituto innovativo delle "clausole contrattuali tipo" riguardanti l'accesso ai dati e il loro utilizzo, che la Commissione europea è incaricata di elaborare e raccomandare ai sensi dell'art. 41 del *Data Act* entro il 12 settembre 2025[101]. Tali clausole modello, volte ad assistere le parti nella stesura e nella negoziazione di contratti equi, ragionevoli e non discriminatori, costituiscono uno strumento di *soft law*[102]. A differenza del controllo sull'abusività, esse non si impongono all'autonomia privata; eppure rivestono un significativo ruolo per l'effettivo raggiungimento degli obiettivi regolatori di cui al *Data Act*: ciò in quanto, in un contesto in cui la prassi negoziale è ancora da costruire, è proprio sulla capacità di tali modelli di orientare l'autonomia privata che si fonda la creazione del relativo mercato[103]. Sin da subito risulta peraltro evidente come l'istituto delle clausole tipo si presti a cooperare con il controllo di abusività, indicando pattuizioni che difficilmente potranno essere qualificate come abusive, rappresentando un parametro di riferimento – pur non vincolante – in un contesto dominato dall'incertezza[104].

Il legislatore europeo apre così nuovi spazi di tutela, che potrebbero fungere da modello anche al di fuori dell'ambito specifico dell'accesso e dell'utilizzo dei dati. Più in generale, questi sviluppi evidenziano, nel complesso, la crescente vocazione del diritto privato europeo a proporsi come strumento fondamentale di regolazione del mercato, ponendo le tecniche civilistiche a servizio delle politiche pubbliche dell'Unione.

---

[101] La versione finale del documento è successiva: cfr. Communication to the Commission, *Approval of the draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contract (with Annexes)*, Brussels, 19.11.2025, C(2025) 7750 final.

[102] V., *amplius*, T. RODRÍGUEZ DE LAS HERAS BALLELL, *Drafting Model Contractual Terms for Voluntary B2B Data Sharing: A Tool to Deal with Unfairness*, in in S. LOHSSE, R. SCHULZE e D. STAUDENMAYER (a cura di), cit., p. 127 ss.

[103] Di qui l'attenzione nel dibattito scientifico, testimoniata dal fatto che i «Model Contract Clauses under the Data Act» costituiscono l'oggetto dell'ultimo *Münster Colloquium* previsto il 27 e 28 novembre 2025, *www.jura.uni-muenster.de/de/fakultaet/fakultaetsnahe-einrichtungen/centrum-fuer-europaeisches-privatrecht/muenster-colloquia-on-eu-law-and-the-digital-economy/*.

[104] In tal senso, tra gli altri, D. STAUDENMAYER, *Der Data Act im Gefüge des europäischen digitalen Privatrechts*, in *NJW*, 2024, p. 1380.

The new balance between data circulation and data protection in the Digital Single Market[*]

di MARCO OROFINO[**]

SUMMARY: 1. Introduction: data as a complex legal asset. – 2. The evolution of the European approach to data free flow. – 3. Beyond protection: the Data Governance Act, the Data Act, the EHDS, and the AI Act. – 4. Regulated data circulation as a constitutional requirement for the Digital Society. – 5. Conclusions.

1. Introduction: data as a complex legal asset

In recent years, data governance has assumed a central role in economic, political and legal debates. Within an increasingly interconnected digital society – further accelerated by the ongoing AI revolution – the availability and the circulation of data can no longer be regarded merely as a technical issue or an economic resource underpinning global or regional markets. Rather data has acquired constitutional significance, as it is intrinsically connected to the effective exercise of fundamental rights.

The central claim advanced here, whereas data regulation was historically conceived and structured around personal data protection as a defensive right – primarily aimed at preventing intrusions into private life – the contemporary challenge lies in developing a governance model that enhances data usage while safeguarding dignity, equality, and individual autonomy. The need for data protection is by no means obsolete, the risks of intrusion into personal choices – and even into the capacity for self-determination – are constantly and dangerously increasing.

Nevertheless, this not diminish the necessity of a paradigm shift in regulatory approach.

This transformation, already significantly advanced, entails completing transition from a proprietary paradigm to one of openness

[*] The reflections developed herein are the outcome of the Net4Future research project carried out within the RESTART programme. The paper has not been subject to peer review, in accordance with the journal's editorial policies and in compliance with the ANVUR criteria set out in Article 2, paragraph 2, letter (c).

[**] Full Professor of Constitutional and Public Law, University of Milan.

grounded in shared responsibility, where algorithmic transparency, infrastructure security, and informed individual participation are paramount.

From a methodological perspective, this study adopts a constitutional lens, examining the evolution of the European legal framework on data through both its regulatory and its rights-based dimension.

The analysis proceeds along two main axes: first, by reconstruction the gradual shift from a defensive model of data protection to a governance-based approach that actively promote data circulation: and second, by assessing why this shift is not merely desirable for reasons of competition or economic efficiency, but constitutionally necessary for effective protection of fundamental rights in the digital society.

The expected outcome of this inquiry is twofold.

On the one hand, it highlights the emergence of a new "constitutional grammar" of data within the European Union, where circulation is no longer conceived solely as an economic tool but as a structural condition for rights. On the other hand, it shows how the Union, through instruments such as the GDPR, the Data Governance Act, the Data Act, the European Health Data Space, and the Artificial Intelligence Act, has assumed a leading role that transcends market regulation and points toward a new phase of European constitutional integration.

2. The evolution of European approach to data free flow

For a long time, the flow of information was regulated at the national level. Each country adopted its own rules governing the management, access, and protection of information held by public or private entities. To simplify this framework, the circulation of information managed by public administrations was restricted and governed by strict legal condition under national administrative law, while the circulation of information held by private parties fell within the scope of private and contract law. In each national legal system, specific restrictions were linked to the implementation of constitutional guarantees concerning privacy.

This fragmented yet broadly shared situation characterized most European countries prior to the intervention of the European Union.

Directive 95/46/EC marked the beginning of a harmonised European framework for the regulation of information flows, with particular

reference to personal data held by public or private entities[1].

Since the European Union is founded on the principle of free movement, the free movement of data emerged as a complementary requirement, ensuring coherence with the broader logic of the internal market.

At the same time, the free flow of data within the Union required a common level of protection, since member States had already begun to intervene unilaterally, thereby introducing barriers and undermining the logic of integration.

The logic of the Directive – at least in the way it was interpreted – was essentially defensive and rested upon a property-based model, exemplified by the primacy of consent among the conditions of lawful processing, the general prohibition on the processing of sensitive data under specific derogation, the enumeration of a series of data subject rights in which the proprietary logic clearly transpired, and the establishment of supervisory authorities focused on oversight.

Notwithstanding certain ideological emphases the approach adopted at that time was more than justifiable. It sought to strike a balance between data protection as fundamental right and data circulation as an economic instrument.

Over time, EU legislation expanded its scope beyond personal data. Subsequent interventions addressed data held by public sector bodies.

A new regulatory season was inaugurated by Directive 2003/98/EC on the re-use of public sector information[2]. It introduced, albeit with significant limitations, the principle of open public data. The main objective was to ensure the availability of data held by public authorities in order to support European businesses. At that stage, the free flow of data was still primarily regarded as an economic tool but it also began to be conceived as a means of fostering transparency and extend the control over the exercise of public powers

The emergence of a new function of the free flow of data become more evident with subsequent acts. Directive 2013/37/EU[3] and Directive (EU)

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995.

[2] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 *on the re-use of public sector information*, OJ L 345, 31.12.2003

[3] Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC *on the re-use of public sector information*, OJ L 175, 27.6.2013.

2019/1024[4] consolidated a culture of reuse grounded in accessibility, interoperability, cost-free availability, and the prioritisation of high-value datasets. These instruments also significantly expanded the scope of open data by narrowing the range of exceptions to disclosure.

Within this context, it should be noted that the new regulatory course continued to exclude personal data. The turning point occurred with the General Data Protection Regulation[5] (GDPR), which marked a genuine paradigm shift as evidenced by its very legal basis: it is grounded not only in Article 114 TFEU but also in Article 16, thereby placing data protection and the promotion of the free flow of data on an equal footing.

As widely emphasised in legal scholarship, the GDPR modernised the personal data framework through instruments such as accountability and co-regulation, privacy by design and by default, and mechanisms for assessing the compatibility between data processing and fundamental rights. More generally, it marked a first shift in the approach. no longer a regulation based on ownership but a regulation based on control.

Attempting to balance protection and circulation, one might say that the GDPR tried to be both a stern schoolmaster and a cheerful enabler. This duality is inherent in a context of shared responsibility, which necessarily requires a combination of flexibility and strict control.

In this broader framework, Regulation (EU) 2018/1807 on the free flow of non-personal data[6] further complemented the GDPR by addressing a different but equally strategic dimension. By prohibiting unjustified data localisation requirements and strengthening portability – particularly for professional users – it contributed to the construction of a genuinely integrated data economy within the Union.

Taken together, the GDPR and the Free Flow of Non-Personal Data Regulation represent the first attempt to design a comprehensive European legal environment in which the circulation of data, whether personal or non-personal, is promoted under conditions that simultaneously safeguard

[4] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 *on open data and the re-use of public sector information* (Open Data Directive), OJ L 172, 26.6.2019.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation, GDPR), OJ L 119, 4.5.2016.

[6] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 *on a framework for the free flow of non-personal data in the European Union*, OJ L 303, 28.11.2018.

fundamental rights and ensure market efficiency. This dual structure laid the foundations for the subsequent legislative season, in which the Union explicitly embraced data as a strategic asset to be governed not only through protection but also through active promotion and valorisation.

3. Beyond protection: the Data Governance Act, the Data Act, the EHDS, and the AI Act

In the most recent phase, a significant wave of new regulations has been approved – among them the Digital Services Act (DSA)[7], the Digital Markets Act (DMA)[8], the Data Governance Act (DGA)[9], the Data Act (DA)[10], the European Heath Data Spaces (EHDS)[11], and the Artificial Intelligence Act (AIA)[12]. All of these acts introduce specific provisions on data circulation, including aspects of personal data circulation, thereby producing effects on the framework established by the GDPR.

While neither the DSA nor the DMA is a regulation on data (personal or non-personal) as such, both pursue the objectives of enhancing transparency and rebalancing the market by curbing excessive concentrations of power arising from data hoarding and exploitation control over data usage, and on the other, curbs the concentration of power arising from data hoarding and exploitation.

By contrast, the other instruments - the Data Governance Act, the Data Act, the European Health Data Spaces and to some extent, also the Artificial Intelligence Act – constitute genuine data regulations, as they establish substantive rules governing the circulation, sharing and re-use of data.

---

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 *on a Single Market for Digital Services* (Digital Services Act), OJ L 277, 27.10.2022.

[8] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 *on contestable and fair markets in the digital sector* (Digital Markets Act), OJ L 265, 12.10.2022.

[9] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 *on European data governance* (Data Governance Act), OJ L 152, 3.6.2022.

[10] 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* (Data Act), OJ L 2023/2854, 22.12.2023.

[11] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 *on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/284*, OJ L, 2025/327, 5.3.2025.

[12] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 *laying down harmonised rules on artificial intelligence* (Artificial Intelligence Act), OJ L 2024/1689, 12.7.2024

Just a few examples illustrate this new approach. The DGA introduces a trust-based model for data sharing, promoting voluntary mechanisms such as data altruism and ensuring the fair re-use of data held by public bodies, including sensitive and personal data, under strict safeguards. It also regulates data intermediaries to foster reliable infrastructures for data access and re-use, laying the foundation for common European data spaces like the European Health Data Space (EHDS). This regulation is highly significant, both for its own objectives and for the argument advanced in this study, as it directly impacts the rules governing the circulation of health data—classified under the GDPR as "sensitive" or "special category" data.

According to Article 9 GDPR, such data may only be processed under one of the exceptions to the prohibition set out in paragraph 2. The EHDS provides a specific legal basis for both the primary and secondary use of health data, thereby moving beyond reliance on individual consent.

The Data Act, with a more private-law orientation, empowers users of connected devices to access and share the data they generate, thereby reinforcing the principle of user control over personal data. These rights are both contractual and rooted in the public interest, as they complement the fundamental right to data protection under the GDPR.

The Act is particularly significant, both for its own objectives and for the argument advanced in this study, since it directly affects the rules governing the circulation of all data—including those falling under the GDPR's special categories of personal data, which are generally subject, pursuant to Article 9, to narrowly defined exceptions to the prohibition of processing.

At the same time, the DA embodies the principle of data circulation as a constitutional requirement, ensuring that information produced in the digital environment does not remain locked within proprietary silos but can circulate under fair and secure conditions, thereby sustaining innovation, market integration, and the effective enjoyment of fundamental rights.

Taken together, the DGA, the DA, and the EHDS—building on the governance model introduced by the DGA—mark a shift from a merely protective approach toward a governance-based framework. This evolution does not simply balance innovation, personal data rights, and societal interests at the regulatory level, but reflects a deeper constitutional reorientation: the circulation of data is recognised as a necessary condition

for the effective enjoyment of fundamental rights in the digital society.

They function as enabling pillars for regulated and secure data circulation, aligned with the GDPR but pushing beyond its protective framework to support Europe's broader goals of digital sovereignty and responsible data economy. Importantly this evolution, in line with the Union's official policy documents, emphasises that the use of data must serve the protection and effective enjoyment of fundamental rights.

The same approach can be found in the AI Act, which establishes a risk-based regulatory model for artificial intelligence. The Act explicitly links this model to both the free movement of AI-based goods and services and the protection of fundamental rights, as emphasised in its recitals[13].

Concrete examples of this favor for data circulation can be found in multiple provisions of the Act, ranging from rules on data governance and dataset quality to those on testing, post-market monitoring, and the functioning of regulatory sandboxes. Article 10 requires high-risk AI systems to rely on high-quality training, validation, and testing datasets under strict conditions, including – where strictly necessary – the processing of sensitive personal data, always subject to appropriate safeguards. Article 59 further permits the use of personal data in regulatory sandboxes for the development, testing, and validation of AI systems, provided this takes place under controlled and lawful conditions. In addition, Article 61 on post-market monitoring obliges providers of high-risk AI systems to collect and analyse operational data after deployment in order to ensure ongoing compliance, thereby reinforcing the principle that data must circulate within secure and accountable frameworks. Similar obligations of documentation and transparency, scattered across other provisions of the Act, equally presuppose and promote the regulated sharing and accessibility of data. Taken together, these provisions demonstrate that the Act adopts a clear pro-circulation stance: since artificial intelligence cannot operate effectively without broad access to and sharing of data, the Union's objective is not to restrict circulation but to promote it within a framework of legality, security, and fundamental rights protection.

[13] See Recital 5 AI Act: «This Regulation aims to improve the functioning of the internal market by laying down a uniform legal framework for the development, the placing on the market, the putting into service and the use of artificial intelligence in conformity with Union values, supporting the free movement of AI-based goods and services across borders…».

4. Regulated data circulation as a constitutional requirement for the Digital Society

The analysis conducted so far suggests that an ongoing shift is taking place from a dichotomic approach - protection versus circulation – to a governance-based model. What remains to be clarified, however, is why such a change is not only desirable in order to promote competition and foster European economy but constitutionally necessary.

The concept of regulated circulation—promoted by recent European regulations—is therefore pivotal: only a system that guarantees accessibility and reusability of data, while respecting principles of security, transparency, and fairness, can support the effective realisation of rights in the digital society

In fields such as healthcare, education, mobility, and digital services, the capacity to access and share data – under clear rules of interoperability, transparency, and security – constitutes the very condition for making rights effectively actionable. While this holds true across all sectors, in some domains its relevance becomes immediately visible.

The protection of fundamental rights has always been technologically bound. We would not, for instance, regard it as compatible with the right to education (art. 14 EU CFR or art. 34 It. Const.) for students to pursue their studies in caves rather than in heated schools or in contemporary terms, even in classrooms devoid of digital tools such an interactive whiteboard. Nor would we consider it compatible with the right to healthcare (Art. 35 EU CFR or art. 32 It. Cost) for a broken leg to be cast without an X-ray, relying solely on clinical judgment or for a cruciate ligament to be operated on without arthroscopy.

The same reasoning applies in other domains. The right to work and fair working conditions (Arts. 15–16 EU CFR; Art. 4 It. Const.) increasingly depends on digital platforms and labour-market data, including systems for matching workers with opportunities and monitoring workplace risks. The right to social security and assistance (Art. 34 EU CFR; Art. 38 It. Const.) presupposes interoperable databases to manage welfare benefits, prevent fraud, and ensure portability of rights across borders. The right to freedom of movement and residence (Art. 45 EU CFR; Art. 16 It. Const.) requires the secure exchange of personal, biometric, and administrative data across Member States to make mobility effective. Even the right to effective judicial protection (Art. 47 EU CFR; Art. 24 It. Const.) increasingly relies on digitalised judicial files,

interoperable case-law databases, and AI-assisted tools that demand structured access to data.

Technology thus reshapes what we understand to be the essential content of a right.

In the health sector, concrete illustrations of the importance of regulated circulation include electronic health records, epidemiological surveillance systems, interoperable databases enabling early diagnosis, personalised treatments, and continuity of care, as well as numerous AI-based applications already available across medical disciplines.

Artificial intelligence technologies, in particular, promise new opportunities and are likely to expand what we consider to be the essential content of fundamental rights. Yet these technologies depend on data – they cannot function effectively without it. This is why the circulation of data is not merely a regulatory matter but ultimately a constitutional one: without meaningful access to data, many fundamental rights risks remaining purely formal rather than substantively guaranteed.

If the circulation of data becomes a precondition for the guarantee of fundamental rights, further constitutional issues inevitably arise. These principles can only be outlined here without the possibility of an extensive discussion, but their relevance to the constitutional nature of data circulation is undeniable.

It is closely linked, first, to the principle of substantive equality (Arts. 20–21 EU CFR; Art. 3(2) It. Const.), which requires the removal not only of legal but also of technological and infrastructural barriers that hinder effective participation in social, political, and economic life. It is also connected to the principle of solidarity (Art. 2 TEU; Arts. 31–34 EU CFR; Arts. 2 and 38 It. Const.), understood as a collective duty to ensure access to the digital tools and data flows that sustain welfare and citizenship. Finally, it resonates with the principle of economic, social, and territorial cohesion (Art. 174 TFEU; implicitly reflected in Arts. 2 and 3 It. Const.), which requires that digital fragmentation and asymmetries in access to data do not exacerbate geographical or socioeconomic divides.

Beyond equality, solidarity, and cohesion, other constitutional concerns may also be mentioned. Among them are the principles of dignity and personal autonomy (Arts. 1 and 8 EU CFR; Art. 2 It. Const.), the protection of freedom of expression and information (Art. 11 EU CFR; Art. 21 It. Const.), the conditions for democratic participation, the principles of proportionality and limitation of public powers (Art. 52 EU

CFR; Art. 97 It. Const.), and finally the right to effective judicial protection (Art. 47 EU CFR; Art. 24 It. Const.).

Each of these principles, although not explored here in detail, is deeply intertwined with the constitutional implications of data circulation.

5. Conclusions

The analysis conducted has sought to demonstrate that the European legal framework on data has undergone a profound transformation: from a defensive model centred on personal data protection, to a governance-based approach in which the circulation of data is actively promoted under regulated conditions. This evolution has been gradual, beginning with the harmonisation introduced by Directive 95/46/EC, consolidated through the GDPR and the Regulation on the free flow of non-personal data, and culminating in the most recent package of measures—the Data Governance Act, the Data Act, the European Health Data Space, and the Artificial Intelligence Act.

What emerges is a new constitutional grammar of data: circulation is no longer conceived merely as an economic tool, but as a precondition for the effective exercise of fundamental rights. Health, education, mobility, and democratic participation increasingly depend on secure, transparent, and fair access to and reuse of data. In this sense, regulated data circulation has become a constitutional necessity, closely tied to principles such as equality, solidarity, and cohesion, and deeply interwoven with dignity, autonomy, freedom of expression, proportionality, and judicial protection.

The European Union's legal order is thus moving beyond the traditional opposition between protection and circulation. It is embracing a model of shared responsibility, in which rights are safeguarded not only by shielding individuals from risks, but also by enabling their substantive enjoyment through structured access to data. This shift entails both opportunities and challenges: ensuring that technological development serves fundamental rights, preventing new inequalities, and avoiding excessive concentrations of informational power.

Ultimately, the constitutional imperative of our digital society is clear: without meaningful, regulated, and secure data circulation, fundamental rights risk remaining purely formal. With it, they can be realised in their full substantive dimension.

In this perspective, the European Union emerges as a constitutional actor in its own right: its intervention in the field of data goes well beyond the regulation of markets, amounting instead to a new step in the process

of European integration. By framing data circulation not merely as an economic resource but as a condition for the effective enjoyment of rights, the Union reshapes the very grammar of constitutional law in the digital age, reinforcing its role as both a guarantor of fundamental rights and a driver of political and social cohesion.

Il *deepfake*: aspetti tecnici, regolamentazione, guerra ibrida ed equilibri geopolitici

di GIOVANNI ZICCARDI*

SOMMARIO: 1. Gli aspetti tecnici. – 2. Gli equilibri democratici. – 3. La regolamentazione. – 4. *Deepfake* e bambini: il documento del Parlamento europeo. – 5. L'azione del Garante per la protezione dei dati italiano: il suo *vademecum*. – 6. Conclusioni e prospettive.

1. Gli aspetti tecnici

Il termine "deepfake" è comunemente utilizzato – sia in ambito tecnico, sia in ambito sociale e politico – per designare un insieme di tecniche che consentono di creare o manipolare contenuti multimediali (immagini, video e tracce audio) attraverso strumenti d'intelligenza artificiale particolarmente avanzati[1].

L'obiettivo finale è quello di generare rappresentazioni estremamente realistiche di persone (reali o inventate che siano) collocate in contesti che possono non corrispondere affatto alla realtà. Si pensi a un viso che pronuncia parole mai dette, a una voce che riproduce un discorso inesistente o a un corpo che compie azioni mai avvenute: tutto questo rientra nel novero dei *deepfake*[2].

L'aspetto più affascinante – e, al contempo, più problematico – è che la manipolazione può essere limitata a un singolo dettaglio, come il movimento delle labbra o il tono della voce, oppure estendersi all'intera scena, trasformando radicalmente la percezione di ciò che si sta guardando o ascoltando[3].

La tecnologia che ha reso possibile questo balzo in avanti nella

* Professore ordinario di filosofia del diritto, presso l'Università degli Studi di Milano.

[1] Per un'introduzione agli impatti sociali e di *governance/policy making* del *deepfake* si veda S. TANEJA, S. GUPTA, M. KUKRETI, E. OZEN (a cura di), *Navigating the Deepfake Conundrum: A Manager's Roadmap*, Cham, 2025. Per un'introduzione giuridica, soprattutto con riferimento agli aspetti patologici, sia consentito il rinvio a G. ZICCARDI, *Dati avvelenati*, Milano, 2024.

[2] Sulle modalità tecniche di creazione dei deepfake si veda Y. MIRSKY E W. LEE, *The Creation and Detection of Deepfakes: A Survey*, in *ACM computing surveys*, 2022-01, Vol. 54 (1), pp. 1-41.

[3] Non è semplice, soprattutto per un giurista, comprendere la sofisticata tecnologia alla base dei *deepfake*. Un buon testo, anche se complesso, è il classico S. RUSSELL e P. NORVIG, *Intelligenza artificiale. Un approccio moderno*, Milano, 2021.

generazione di contenuti sintetici è quella delle *Generative Adversarial Networks* (GAN), introdotte per la prima volta nel 2014[4]. Si tratta di un'architettura innovativa di reti neurali che opera in una sorta di "competizione interna": da un lato vi è una rete "generatrice", il cui compito è creare contenuti sempre più convincenti; dall'altro vi è una rete "discriminatrice", incaricata di distinguere tra ciò che è autentico e ciò che è artificiale e di perfezionare il più possibile il risultato falso.

Il processo si sviluppa come una partita a scacchi in cui, a ogni mossa, il generatore tenta di "ingannare" il discriminatore, mentre quest'ultimo affina continuamente la propria capacità di smascherare il falso[5].

Con il tempo, questa procedura produce un effetto sorprendente: i contenuti sintetizzati diventano talmente *realistici* da confondersi con quelli originali, segnando un passo decisivo verso quella che molti studiosi chiamano, ormai, la "post-verità digitale"[6].

Il risultato di questo "ecosistema tecnologico" è un realismo in costante crescita: la qualità delle immagini, la fedeltà delle espressioni facciali, la precisione del movimento oculare, la coerenza dell'illuminazione e delle ombre rendono i contenuti sintetici sempre più indistinguibili da quelli reali.

Ciò che un tempo richiedeva strumenti avanzati e competenze di nicchia oggi può essere ottenuto con relativa facilità, spesso con software accessibili o, addirittura, con applicazioni commerciali alla portata di utenti non esperti.

Tuttavia, nonostante questo progresso vertiginoso, i *deepfake* non sono privi di imperfezioni.

Gli esperti di investigazioni digitali hanno individuato diversi indizi che, se analizzati con attenzione, possono tradire l'origine artificiale di un contenuto: piccole incoerenze nella *texture* della pelle, movimenti oculari innaturali, errori di sincronizzazione tra labbra e voce, discrepanze

---

[4] Per un approfondimento tecnico sulle GAN si veda X. MAO E Q. LI, *Generative Adversarial Networks for Image Generation*, Singapore, 2021; si veda, anche, S. KADDOURA, *A Primer on Generative Adversarial Networks*, Cham, 2023.

[5] Per comprendere il funzionamento di questo passaggio, si veda J. LANGR E V. BOK, *GANs in action: deep learning with generative adversarial networks*, New York, 2019.

[6] Con riferimento all'idea di post-verità si veda, *inter alia*, G. RIVA, *Fake news: vivere e sopravvivere in un mondo post-verità*, Bologna, 2018. Si vedano, anche: A. GIORDANO, *Democrazia, propaganda, "fatti alternativi", George Orwell e le radici della post-verità*, in *Storia del pensiero politico*, 2022 (3), p. 449-464; L. PELLIZZONI, *Autorità in declino?: L'expertise scientifica nell'epoca della post-verità*, in *Quaderni di Sociologia*, 2021-01, Vol. 86- LXV (86- LXV), pp. 133-152.

nell'illuminazione sono soltanto alcune delle "tracce" che algoritmi di rilevamento – basati, a loro volta, su tecniche di intelligenza artificiale – possono sfruttare per smascherare la falsificazione[7].

In questo equilibrio dinamico tra creazione e rilevazione, tra verosimiglianza e autenticità, si gioca probabilmente oggi una delle partite giuridiche e sociali più complesse e decisive dell'era digitale.

2. Gli equilibri democratici

Se il lato tecnico dei *deepfake* affascina per la potenza dell'innovazione, è nel loro impatto sociale e politico che il giurista può misurare la vera portata di questa tecnologia.

L'idea che un contenuto digitale possa riprodurre con estrema verosimiglianza parole mai pronunciate o azioni mai compiute apre, infatti, scenari dirompenti per l'informazione e per la democrazia stessa[8].

In un'epoca in cui la velocità della comunicazione supera di gran lunga la capacità di *verificarne la veridicità*, i *deepfake* diventano strumenti potenzialmente esplosivi nelle mani di chi mira a manipolare l'opinione pubblica.

Uno dei rischi più evidenti è quello della *disinformazione politica*[9]. Immagini o video che raffigurano *leader* o figure istituzionali mentre pronunciano frasi mai dette, o assumono posizioni inesistenti, possono circolare in rete in poche ore, generando sfiducia verso i media e alimentando la percezione che "nulla sia più vero" nell'intero ecosistema informativo.

Non è difficile immaginare come, in periodi di campagna elettorale, anche un singolo *deepfake* ben confezionato possa spostare l'attenzione mediatica, orientare dibattiti e alimentare sospetti e polarizzazioni. Ciò che rende la minaccia particolarmente insidiosa è la combinazione di realismo

[7] Si veda, sul punto, L. VERDOLIVA, *Media Forensics and DeepFakes: An Overview*, in *IEEE journal of selected topics in signal processing*, 2020-08, Vol. 14 (5), pp. 910-932; Y. MIRSKY E W. LEE, *The Creation and Detection of Deepfakes: A Survey*, in *ACM computing surveys*, 2022-01, Vol. 54 (1), pp. 1-41.

[8] Sul rapporto tra falso digitale e (tenuta della) democrazia si veda M. PAWELEC, *Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions*, in *Digital society: ethics, socio-legal and governance of digital technology*, 2022-09, Vol. 1 (2), p. 19, Article 19; D. CAVEDON-TAYLOR, *Deepfakes and Democracy: A Catch-22?*, in *Journal of the American Philosophical Association*, 2025-09, Vol. 11 (3), pp. 447-466; A. RAY, *Disinformation, deepfakes and democracies: The need for legislative reform*, in *University of New South Wales Law Journal*, 2021-09, Vol. 44 (3), pp. 983-1013.

[9] Sul punto si veda L. W. BENNETT, *The disinformation age: politics, technology, and disruptive communication in the United States*, Cambridge, 2020.

tecnologico e *viralità* dei social media: anche quando il contenuto falso viene smascherato, l'impatto emotivo e reputazionale è spesso irreversibile[10].

La questione s'intreccia, poi, con il fenomeno della *polarizzazione sociale*[11]. In un contesto già segnato da divisioni ideologiche e dalla tendenza a informarsi solo attraverso canali che confermano le proprie convinzioni, i *deepfake* agiscono come amplificatori di ostilità e diffidenza. La diffusione di contenuti falsi può rafforzare narrazioni estremiste, consolidare pregiudizi, creare veri e propri "nemici immaginari" a cui attribuire responsabilità o colpe inesistenti[12].

Il problema, però, non riguarda soltanto la sfera politica e collettiva.

I *deepfake* possono essere usati come armi di *odio interpersonale* o per finalità di diffamazione privata, colpendo persone comuni e trascinandole in scandali artificiali. Un video manipolato che mostra un individuo in atteggiamenti imbarazzanti o compromettenti può distruggere reputazioni, carriere e relazioni personali, con effetti psicologici devastanti. L'accessibilità crescente di queste tecnologie fa sì che oggi non siano più solo governi o grandi organizzazioni a poter manipolare immagini e voci, ma anche singoli individui mossi da rancore, vendetta o semplice intento goliardico. Si parla a volte di "armamento mediatico" dei *deepfake*, a sottolineare come la loro funzione possa trasformarsi in vera e propria arma di propaganda.

In contesti geopolitici delicati, nella diplomazia internazionale o nei conflitti armati, la possibilità di fabbricare prove-video di eventi mai avvenuti introduce rischi per la stabilità globale, alimentando quella che molti studiosi definiscono "guerra dell'informazione".

Sul piano etico, infine, emergono questioni profonde legate al *consenso* e al rispetto della *dignità* personale. Utilizzare l'immagine o la voce di qualcuno senza autorizzazione non è soltanto una violazione della *privacy*, ma tocca il cuore stesso del diritto all'identità e all'autodeterminazione informativa. Ognuno dovrebbe poter controllare la diffusione del proprio volto, della propria voce, del proprio corpo digitale; eppure, il *deepfake* erode questo diritto, privando l'individuo della

---

[10] Ho trattato questo tema, con particolare riferimento ai contenuti politici, in G. ZICCARDI, *Tecnologie per il potere*, Milano, 2019.

[11] Si veda R. BARNES, *Fandom and Polarization in Online Political Discussion: From Pop Culture to Politics*, Cham, 2022.

[12] Sul punto sia consentito il rinvio a G. ZICCARDI, *Online Political Hate Speech in Europe*, Cheltenham, 2020.

possibilità di decidere come e dove la sua immagine viene utilizzata.

In questo intreccio di disinformazione, propaganda, odio e violazione dei diritti personali si gioca il delicato equilibrio tra innovazione tecnologica e protezione dei valori democratici. Il *deepfake*, nato come espressione di creatività e sperimentazione tecnica, rischia di trasformarsi in uno degli strumenti più destabilizzanti dell'era digitale, capace di erodere alla radice la fiducia collettiva nella verità delle immagini e delle parole.

Allo stesso tempo, la *guerra ibrida* è, proprio in questi giorni, un concetto strategico che combina forme convenzionali di conflitto (forze militari, operazioni sul terreno) con metodi non convenzionali: operazioni cibernetiche, disinformazione, interferenza politica, atti di sabotaggio, uso di attori statali e non statali che operano in modo flessibile e spesso nascosto. L'obiettivo di queste strategie miste è destabilizzare il nemico, influenzare gli avversari e la popolazione civile, ottenere vantaggi senza dover sempre utilizzare la forza militare diretta, e spesso con la possibilità di negare o ridurre la responsabilità diretta[13].

Nel contesto della guerra ibrida, i *deepfake* rappresentano una nuova arma dell'informazione, capace di generare contenuti persuasivi – e, spesso, ingannevoli – che possono influenzare le percezioni, i comportamenti e la fiducia pubblica. Possono servire per delegittimare istituzioni, seminare panico, far apparire come verità eventi falsi, e così via. La combinazione di *deepfake* con campagne di disinformazione, *hacking*, manipolazione sui social media rende il quadro particolarmente intricato e pericoloso[14].

Nel conflitto iniziato su larga scala nel 2022 tra Russia e Ucraina, la guerra ibrida con l'uso di *deepfake* è emersa quasi immediatamente. Un esempio significativo è il video *deepfake* (poco sofisticato, ma con un grande impatto simbolico) che mostrava il presidente ucraino Zelenskyy presumibilmente intento a proclamarsi sconfitto, a fuggire da Kiev o a chiedere la resa. In quel caso, il *deepfake* fu diffuso da attori pro-russi che hackerarono il sito di un media ucraino. Sebbene il video fosse rapidamente segnalato come falso, la sua circolazione ebbe l'effetto di

---

[13] Su questo tema si veda M. WEISSMANN (a cura di), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, Londra, 2021; M. E. KAMBOURIS, *Hybrid Warfare 2.2: Where Biothreats Meet Irregular Operations and Cyber Warriors in the 21st Century*, Cham, 2024.

[14] Sul punto si veda F. HANY, *The Weaponization of Deep Fakes*, in *The journal of intelligence, conflict, and warfare*, 2021-11, Vol. 4 (2).

confondere parte dell'opinione pubblica, generare sussurri di smobilitazione, e mettere in discussione la solidità delle comunicazioni ufficiali.

Altri esempi includono l'uso di immagini sintetiche generate da intelligenze artificiali per rappresentare scene di bambini in uniforme militare, eventi tragici falsi o attribuiti erroneamente alle parti in causa, oppure audio manipolato che attribuisce a certi leader dichiarazioni che non hanno fatto[15]. L'obiettivo è spesso duplice: da un lato indebolire il morale interno del nemico, dall'altro creare divisione internazionale o criticità nei Paesi che sostengono l'aggressore.

Un aspetto interessante è che la "difesa" da questi attacchi non è solo militare, ma riguarda anche aspetti di *resistenza cognitiva*: l'alfabetizzazione digitale, il *fact-checking*, la capacità dei media e delle istituzioni di reagire rapidamente e affermare la verità.

Anche nel conflitto Israele-Hamas, l'impiego di *deepfake* si è manifestato come parte della guerra dell'informazione. Fin dall'inizio, si è assistito a una proliferazione di immagini e video manipolati, alcune volte con l'evidente intento di attribuire responsabilità per atrocità non avvenute, o di rappresentare scene di distruzione, sofferenza o urgenza in modo amplificato o falsato.

Un caso citato di frequente è quello di un'immagine, ampiamente diffusa, che mostrava un bambino tra le macerie di Gaza; tale immagine è stata in realtà generata da tecnologia basata su intelligenza artificiale e si è rivelata essere stata utilizzata già in contesti precedenti. Ciò ha generato proteste, manifestazioni e utilizzi simbolici nelle campagne mediatiche, anche internazionali, come in manifestazioni, giornali o social media. La rapidità con cui questi contenuti vengono adottati come "prove" contribuisce a costruire narrazioni con forte impatto emotivo, anche se spesso false.

Un altro elemento da considerare è che la vasta mole di contenuti sospetti costringe giornalisti e istituzioni a spendere *risorse rilevanti* per verifiche, mentre molti utenti comuni condividono senza verificare, amplificando il potenziale danno. E inoltre, la presenza di *deepfake* rende più difficile fare distinzione tra ciò che è autentico e ciò che non lo è in tempi rapidi, elemento fondamentale in situazioni di crisi o conflitto[16].

---

[15] Si veda Z. KHANJANI, G. WATSON E V. P. JANEJA, *Audio deepfakes: A survey, in Frontiers in big data*, 2023-01, Vol. 5, p. 1001063.

[16] Si veda V. W. PICKARD, *Democracy without journalism?: confronting the misinformation society*, New York, 2020.

Questi casi mostrano come il *deepfake* non sia solo un elemento di propaganda: è parte integrante di *strategie ibride* che miscelano conflitto militare, pressione mediatica, influenza internazionale e disinformazione. L'uso di *deepfake* non è isolato, ma spesso combinato con altri strumenti: attacchi informatici, *bot* sui social media, campagne coordinate che sfruttano algoritmi di raccomandazione per aumentare la diffusione.

La scala del problema risiede nella facilità con cui materiale artificiale convincente può essere prodotto e diffuso, nell'impatto emotivo che ha sulle persone e nella difficoltà che le istituzioni hanno di rispondere con la stessa prontezza e credibilità. In guerra, il "momento della verità" spesso perde terreno contro il "momento della percezione": ciò che la gente crede diventa più rilevante di ciò che è reale.

3. La regolamentazione

L'idea di una disciplina efficace che possa regolamentare il fenomeno dei *deepfake* nasce, a nostro avviso, dall'intreccio di (almeno) quattro esigenze: *i)* prevenire la disinformazione e l'abuso dell'immagine altrui, *ii)* garantire rimedi rapidi e proporzionati alle vittime, *iii)* preservare la libertà di espressione e, infine, *iv)* creare incentivi tecnici alla tracciabilità del contenuto sintetico.

L'architettura regolatoria che va emergendo nel mondo combina, a tal fine, strumenti penali e civili, obblighi di trasparenza[17] e di marcatura dei contenuti, doveri per le piattaforme e standard tecnici di "content provenance", ossia di verifica della provenienza di un determinato contenuto.

In questo mosaico, l'Italia ha imboccato, proprio in questi giorni, la via dell'incriminazione autonoma, gli Stati Uniti d'America stanno sperimentando soluzioni settoriali e rispettose dei principi costituzionali, la Cina ha costruito un quadro di controllo e di sicurezza nazionale e l'Unione europea ha innestato il tema nella più ampia cornice orizzontale dell'*AI Act*, il recente Regolamento sull'intelligenza artificiale[18].

In Italia, in particolare, la recente legge sull'intelligenza artificiale del

[17] Si veda H. LU, S. YUAN, *"I know it's a deepfake": the role of AI disclaimers and comprehension in the processing of deepfake parodies*, in "Journal of communication", 2024-10, Vol. 74 (5), pp. 359-373.

[18] Si veda M. J. BLOCK, *A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union*, in *Journal of European Consumer and Market Law*, 2024-08, Vol. 13 (4), pp. 184-192; si veda anche M. ŁABUZ, *Deep fakes and the Artificial Intelligence Act - An important signal or a missed opportunity?*, in Policy and Internet, 2024-12, Vol. 16 (4), pp. 783-800.

25 settembre 2025 ha portato all'introduzione dell'art. 612-*quater* c.p., che punisce la "illecita diffusione di contenuti generati o manipolati con sistemi di intelligenza artificiale" quando idonei a ingannare e arrecare danno, con pene da uno a cinque anni[19].

Si legga il testo del nuovo articolo 612-quater: «Art. 612-quater. – (Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale) – Chiunque cagiona un danno ingiusto ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e idonei a indurre in inganno sulla loro genuinità, è punito con la reclusione da uno a cinque anni.

Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate».

La scelta del nostro legislatore ci appare chiara: tipizzare il *deepfake* come condotta autonoma, così da coprire lacune non sempre colmabili dalle fattispecie tradizionali (diffamazione, sostituzione di persona o trattamento illecito di dati). La discussione parlamentare ha anche toccato misure complementari, come obblighi di etichettatura e responsabilità di segnalazione e rimozione in capo alle piattaforme, disegnando un quadro ibrido necessario tra diritto penale e regolamentazione dei servizi digitali che cerca di controllare le dinamiche, rapidissime, della circolazione online di simili contenuti.

Negli Stati Uniti d'America, dove il Primo Emendamento impone un vaglio severo sulle restrizioni ai contenuti, i legislatori statali hanno scelto quasi sempre approcci mirati. Non ci è possibile, in questa sede, elencare tutte le proposte di legislazione federale e locale, che sono oltre quaranta. La California, però, è stato il primo laboratorio di riferimento[20]. Nel 2019 un provvedimento ha limitato, ad esempio, l'uso di *deepfake* ingannevoli in prossimità delle *elezioni*, ma la norma era temporanea ed è stata oggetto di forti critiche: sarebbe stata di difficile applicazione e con un rischio di estendersi anche a contenuti ammissibili nell'agone politico. Nel medesimo anno, sempre in California, un secondo provvedimento ha

[19] Sul rapporto tra norma penale e *deepfake* si veda I. ČUČILOVIĆ, *Deepfake technology: Criminal law implications*, in *Crimen*, 2024-01, Vol. 15 (3), pp. 325-342.
[20] Si veda M. BODI, *The First Amendment Implications of Regulating Political Deepfakes*, in *Rutgers Computer & Technology Law Journal*, 2021-03, Vol. 47 (1), p. 143.

introdotto la possibilità di una causa civile di risarcimento per i *deepfake* sessuali non consensuali, aprendo la strada a rimedi risarcitori mirati. Più di recente, nel 2024, il Governatore Newsom ha proposto un pacchetto di misure normative per contrastare la disinformazione elettorale generata da intelligenza artificiale che mirano a rafforzare gli obblighi di rimozione e d'informazione per le grandi piattaforme nei 120 giorni precedenti al voto. Tuttavia, la regolamentazione giuridica rimane un terreno accidentato: in molti ravvisano probabili violazioni del Primo Emendamento.

Il risultato è, in molti Stati, un quadro dinamico, efficace sul piano simbolico e talvolta pratico, ma costantemente messo alla prova dal bilanciamento tra tutela dell'integrità del dibattito pubblico e libertà di parola.

La Cina, si diceva, ha imboccato una strada diversa, di taglio più burocratico-amministrativo e preventivo: le prime norme sulla *Deep Synthesis* sono entrate in vigore il 10 gennaio 2023 e impongono obblighi stringenti ai fornitori di servizi di dati sintetici, tra cui identificazione degli utenti, valutazioni di sicurezza, etichettatura chiara del contenuto sintetico e divieti specifici quando l'uso può ingannare o perturbare l'ordine nel mondo dell'informazione.

Nel 2025, nuove regole di etichettatura per i contenuti generati da intelligenza artificiale hanno ulteriormente precisato obblighi "espliciti" e "impliciti" di segnalazione, puntando a rendere *riconoscibile* la provenienza artificiale di simili contenuti lungo la filiera. Questo assetto, innervato nell'ecosistema regolatorio digitale cinese, mira meno, come è chiaro, alla sanzione penale in senso stretto e più al controllo *ex ante* degli attori e dei flussi informativi[21].

Sullo sfondo, l'Unione europea ha scelto di disciplinare i *deepfake* all'interno dell'*AI Act*, come tassello di un *framework* tecnologicamente neutro e "risk-based".

Il punto fondamentale, nel testo del regolamento, è il capo IV sulla trasparenza (Articolo 50 e seguenti): i sistemi che generano, o manipolano, contenuti sintetici devono assicurare che gli utenti siano informati della

[21] Sul punto si veda E. HINE, L. FLORIDI, *New deepfake regulations in China are a tool for social stability, but at what cost?*, in *Nature machine intelligence*, 2022-07, Vol. 4 (7), pp. 608-610; G. ZHENG, J. SHU, K. LI, *Regulating deepfakes between Lex Lata and Lex ferenda—a comparative analysis of regulatory approaches in the U.S., the EU and China*, in *Crime, law, and social change*, 2025-06, Vol. 83 (1), p.1, Article 1; G. DE SETA, *Huanlian, or changing faces: Deepfakes on Chinese digital media platforms*, in *Convergence*, 2021-08, Vol. 27 (4), pp. 935-953.

natura artificiale del contenuto e devono adottare misure tecniche idonee alla marcatura, in modo da conservarne l'origine lungo catene di riuso e ricondivisione.

La norma, oggi collocata nell'Articolo 50 dedicato agli obblighi di trasparenza, specifica che l'indicazione deve essere *chiara* e *comprensibile*, con eccezioni circoscritte per la ricerca, l'applicazione forense o la prevenzione di reati, purché siano previste garanzie adeguate.

Il legislatore europeo qualifica queste tecnologie come *limited-risk* sul piano sistemico, ma impone obblighi di *disclosure* e *labeling* che diventano particolarmente rilevanti quando il contenuto può incidere su diritti fondamentali, processi elettorali e ordine pubblico.

Analizzando con cura l'Articolo *de quo*, ne possiamo ricavare, "a cascata", alcune linee di *policy* utili anche per orientare il dibattito nazionale: *i)* la possibilità di introdurre un obbligo generalizzato di etichettatura per i contenuti sintetici, con standard tecnici interoperabili che favoriscano la verificabilità; *ii)* il prevedere rimedi civili rapidi e ordini di rimozione "mirati e tempestivi" per i casi di danno individuale (in particolare si pensi ai *deepfake* a sfondo sessuale non consensuali); *iii)* il calibrare l'intervento del diritto penale solo sulle condotte di maggiore offensività sociale (frodi portare da gruppi organizzati, profitto, destabilizzazione del processo democratico); *iv)* il responsabilizzare gli intermediari con procedure trasparenti di *notice and action* e con doveri rafforzati in periodi elettorali; *v)* l'investire nella *media literacy* e nella capacità forense di riconoscimento, perché la regolazione è efficace solo se sostenuta da competenze diffuse e da strumenti tecnici adeguati.

In questo senso, il dialogo in corso che abbiamo raccontato, seppur sommariamente, tra la tipizzazione italiana, le soluzioni californiane, il modello amministrativo cinese e la cornice europea dell'*AI Act* suggerisce un *approccio multilivello*: diritti e rimedi per le persone, governance e conformità per i fornitori, trasparenza e marcatura come "lingua franca" dell'ecosistema informativo.

4. *Deepfake* e bambini: il documento del Parlamento europeo

Un recente *briefing* del Parlamento europeo (EPRS, 2025) ha introdotto alcuni aspetti interessanti, e in larga parte inediti, sul fenomeno dei *deepfake*, con particolare attenzione alla protezione dei *minori* e alla sua rapida evoluzione tecnologica.

La diffusione, si legge nel documento, è ormai esponenziale: si stima che nel 2025 saranno condivisi online circa *otto milioni* di *deepfake*, contro

i cinquecentomila del 2023, con l'Europa che prevede che entro il 2026 fino al 90 % dei contenuti online potrebbe essere generato *sinteticamente*.

L'elemento più allarmante, nei dati riportati, è che il 98 % dei *deepfake* ha natura *pornografica* e che una quota crescente coinvolge minori, alimentando fenomeni come *sextortion*, *nudify apps*, *grooming* e cyberbullismo.

La creazione di materiale pedopornografico sintetico (CSAM)[22] con tecniche di *generative AI* rappresenta oggi una priorità assoluta per Europol e Interpol, poiché queste immagini – spesso indistinguibili da quelle reali – vengono usate per adescare, ricattare o portare violenza psicologica a minori, con gravi impatti personali e giuridici.

Il documento segnala anche la crescita del fenomeno del *voice phishing* ("vishing"), reso possibile dall'uso di campioni vocali di vittime raccolti online per generare clonazioni quasi perfette, utilizzate in frodi, estorsioni e impersonificazioni in tempo reale, talvolta durante *video-call deepfake* che hanno già prodotto perdite finanziarie milionarie.

Inoltre, la capacità di distinguere contenuti reali e sintetici rimane *bassissima*: anche gli esperti di nuove tecnologie identificano erroneamente oltre il 60 % dei contenuti generati da intelligenza artificiale come autentici, e un quarto degli adulti riferisce di aver subìto o di aver conosciuto qualcuno colpito da truffe vocali basate su *deepfake*.

Sul piano normativo, il briefing evidenzia che diversi Stati membri dell'Unione europea stanno già aggiornando le proprie leggi per includere espressamente i *deepfake* sessuali e il CSAM sintetico tra i reati perseguibili. Tuttavia, permangono difficoltà nel rendere interoperabili le soluzioni di *watermarking* e *content provenance* tra operatori privati e legislazioni nazionali, così come nel garantire l'efficacia delle tecniche di *detection*, che oggi si trovano a dover inseguire modelli generativi in continua evoluzione.

Infine, il documento insiste sulla necessità di una *AI Literacy* mirata per minori, genitori e insegnanti, insieme a strumenti educativi *safe-by-design* e a una governance tecnologica che coinvolga piattaforme, scuole,

[22] Sul tema si veda D. KING, R. SLIKBOER, M. HENSHAW, D. MEYER, J. R. P. OGLOFF, *Unmasking the Men Who Produce Child Sexual Abuse Material (CSAM): Criminal Diversity and Sociodemographic Characteristics*, in *Sexual Abuse*, 2025-09, p. 10790632251377705; J. ENDE, *Don't throw the baby out with the bathwater: Protecting children against CSAM deepfakes without banning ai technology*, in *Family Court Review*, 2025-04, Vol. 63 (2), pp. 324-338; S. EELMAA, *Sexualization of children in deepfakes and hentai*, in *Trames*, 2022-06, Vol. 26 (2), pp. 229-248.

autorità di protezione dati e Forze dell'Ordine, così da affrontare in modo coordinato la dimensione sociale, psicologica e giuridica del problema.

5. L'azione del Garante per la protezione dei dati italiano: il suo *vademecum*

Nel dicembre 2020 il Garante per la protezione dei dati personali ha pubblicato un vademecum dedicato ai rischi del *deepfake*, con l'obiettivo di sensibilizzare cittadini e istituzioni su una tecnologia che sta rapidamente conquistando, anche in Italia, l'ecosistema digitale, con conseguenze imprevedibili.

Il documento muove da una definizione chiara: il *deepfake* è un falso digitale generato dall'intelligenza artificiale che può "rubare" la faccia, la voce e, persino, l'identità delle persone.

Grazie a sofisticati algoritmi di *deep learning*, contenuti reali possono essere manipolati fino a ricostruire espressioni, parole e comportamenti mai avvenuti, con un realismo tale da ingannare non solo l'osservatore comune ma, in alcuni casi, anche sistemi tecnologici di sicurezza basati su *dati biometrici*.

Il Garante sottolinea come la diffusione di applicazioni sempre più accessibili, capaci di generare video sofisticati con un semplice *smartphone*, stia trasformando i *deepfake* da strumenti costosi e di nicchia a *tecnologie di massa*. E con questa sorta di "democratizzazione" arrivano i rischi più gravi: perdita di controllo sull'immagine personale, possibilità di essere rappresentati in contesti offensivi o compromettenti, manipolazioni a scopo diffamatorio o ricattatorio. In altre parole, i *deepfake* minacciano quella che il documento definisce *autodeterminazione informativa*, ossia il diritto di ogni individuo a decidere cosa condividere di sé e in quali contesti[23].

Il vademecum dedica, inoltre, ampio spazio a fenomeni particolarmente preoccupanti come il cosiddetto "deepnude"[24], dove i volti – a volte di minori – vengono montati su corpi nudi o inseriti in scene

[23] Sul concetto di "autodeterminazione informativa", soprattutto nell'ambito della salute, si veda J. MONDUCCI, *Il dato genetico tra autodeterminazione informativa e discriminazione genotipica*, Bologna, 2014. Sulla difficoltà di "autodeterminarsi" nella società digitale delle attuali piattaforme (anche con riferimento alle relazioni sociali) si veda G. PISANI, *Piattaforme digitali e autodeterminazione*, Modena, 2023.

[24] Sul tema della pornografia generata dalla intelligenza artificiale si veda V. A. LAPOINTE, S. DUBÉ, S. RUKHLYADYEV, T. KESSAI, D. LAFORTUNE, *The Present and Future of Adult Entertainment: A Content Analysis of AI-Generated Pornography Websites*, in *Archives of sexual behavior*, 2025-03.

sessualmente esplicite, alimentando fenomeni di *revenge porn*[25] e pornografia illegale[26]. Ma i *deepfake* possono anche diventare strumenti di cyberbullismo, di estorsione o di manipolazione politica, diffondendo *fake news* attraverso immagini apparentemente autentiche di leader o personaggi pubblici.

Non mancano rischi sul fronte della *sicurezza informatica*: i volti e le voci artefatti possono essere usati per truffe, furti di identità, attacchi di phishing e persino per aggirare sistemi di autenticazione biometrica, sempre più diffusi in ambito bancario, sanitario e nella domotica. Sebbene oggi la tecnologia di protezione riesca ancora a contenere queste minacce, il Garante avverte che l'evoluzione dei *deepfake* potrebbe presto cambiare gli equilibri, rendendo le *intrusioni* più sofisticate e difficili da individuare.

Accanto ai rischi, il documento indica anche, opportunamente, le prime strategie di difesa.

Le grandi piattaforme digitali stanno sperimentando algoritmi di rilevamento e sistemi di segnalazione, mentre le autorità di protezione dati possono intervenire quando vi siano violazioni della *privacy* o della normativa penale.

Tuttavia, la prima linea di protezione resta la *consapevolezza degli utenti*: limitare la diffusione incontrollata di immagini personali, imparare a riconoscere gli indizi tecnici di un possibile *deepfake* – movimenti innaturali, ombre incoerenti, deformazioni delle labbra – evitare la condivisione di contenuti sospetti e rivolgersi alle autorità competenti in caso di abuso sono azioni essenziali per contenere il fenomeno.

Il *vademecum* del Garante, con un linguaggio chiaro ma rigoroso, ricorda, in conclusione, che la sfida ai *deepfake* non è solo normativa o tecnologica: è *culturale*. Richiede alfabetizzazione digitale, strumenti giuridici aggiornati e una responsabilità diffusa, capace di coniugare libertà di espressione, tutela della dignità e protezione della verità

---

[25] Sul *revenge porn* attuato anche con strumenti tecnologici si veda A. SORGATO, *Revenge porn. Aspetti giuridici, informatici e psicologici*, Milano, 2019. Sul ruolo delle vittime si veda F. FLORIO, *Non chiamatelo revenge porn*, Milano, 2022. Sui profili psicologici, si veda C. MENTO E F. PIRA, *La violenza in un "click". Profili sociologici, psicologici e giuridici del revenge porn*, Milano, 2023.

[26] Sul tema si veda T. PERCIVAL JAMES, *Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and Federal Law's Current Failure to Protect Vict*ims, in *Brigham Young University Law Review*, 2025-07, Vol. 50 (4), pp. 1159-1190; C. OKOLIE, *Artificial Intelligence-Altered Videos, Image-Based Sexual Abuse, and Data Privacy Concerns*, in *Journal of International Women's Studies*, 2023-03, Vol. 25 (2).

nell'ecosistema informativo contemporaneo.

6. Conclusioni e prospettive

Il fenomeno dei *deepfake*, abbiamo descritto poco sopra, si colloca al crocevia di *tre rivoluzioni parallele*: *a)* quella tecnologica, che con le reti neurali generative – *in primis* le GAN – ha reso possibile la creazione di immagini, voci e video indistinguibili dalla realtà; *b)* quella sociale e politica, che vede nella disinformazione[27] e nell'erosione della fiducia pubblica[28] due minacce senza precedenti per le democrazie contemporanee; e, *c)* quella giuridica, che deve ora confrontarsi con una sfida regolatoria in continua evoluzione, in cui norme nazionali, iniziative sovranazionali e linee-guida etiche cercano di rincorrere l'innovazione tecnologica senza soffocarla[29].

Se, dal lato tecnico, i progressi sono impressionanti, con la capacità delle reti neurali di apprendere e replicare caratteristiche umane in modo sempre più credibile, sul piano sociale le implicazioni diventano di giorno in giorno più allarmanti: la manipolazione di contenuti può minare la veridicità dell'informazione, condizionare elezioni, alimentare campagne di odio e diffamazione[30], ridisegnare in modo arbitrario la reputazione di individui e istituzioni. Il tutto avviene in un ecosistema digitale in cui la velocità di diffusione supera di gran lunga la capacità di verifica, amplificando l'impatto emotivo del falso a scapito della sua successiva smentita.

La risposta normativa, in Europa come in Italia, si sta rapidamente consolidando. L'*AI Act*, con i suoi obblighi di trasparenza e *labeling* ("etichettatura"), disegna una cornice comune che mira a responsabilizzare gli operatori e a proteggere i diritti fondamentali, mentre a livello nazionale leggi specifiche sull'intelligenza artificiale e interventi dell'Autorità

[27] Si veda M. DORATO, *Disinformazione scientifica e democrazia*, Milano, 2019; per una ricostruzione storica si veda T. RID, *Misure attive. Storia segreta della disinformazione*, Roma, 2022. Sul rapporto con la democrazia, si veda A. NICITA, *Il mercato delle verità*, Bologna, 2021. Sul tema delle informazioni tossiche si veda G. SUFFIA, *Pulire l'infosfera. Intelligenza artificiale e contrasto alla disinformazione*, Milano, 2022.

[28] Sul tema della fiducia nella sfera pubblica (e la sua erosione) si veda A. PUGLIESE, *Fiducia ed Etica Pubblica*, Roma, 2021. Con particolare riferimento alla fiducia del cittadino nei confronti delle amministrazioni si veda A. BIANCONI, *Fiducia. Il senso della funzione pubblica tra etica e competenza*, Rimini, 2019.

[29] Per un quadro delle regolamentazioni internazionali sia consentito un rinvio a: G. ZICCARDI, *Diritti digitali*, Milano, 2022.

[30] Sul punto sia consentito il rinvio a G. ZICCARDI, *L'odio online*, Milano, 2016. Con riferimento all'odio in politica: G. ZICCARDI, *Tecnologie per il potere*, Milano, 2019; G. ZICCARDI, *Online political hate speech in Europe*, Cheltenham, 2020.

Garante per la *privacy* rafforzano la tutela penale e amministrativa. Tuttavia, tra norme scritte e realtà operativa permane una *distanza* che non può essere colmata unicamente dal diritto: occorrono tecnologie di rilevazione affidabili, standard internazionali di marcatura dei contenuti, procedure di "notice and action" rapide e sistemi educativi capaci di promuovere un'alfabetizzazione digitale su larga scala[31].

Il futuro richiede dunque un *approccio multilivello*, in cui diritto, tecnologia e cultura interagiscono in modo coordinato.

Serve una regolazione che non sia soltanto repressiva, ma anche preventiva e formativa; servono strumenti tecnici che sappiano identificare e segnalare i contenuti manipolati senza ostacolare la libertà creativa o la ricerca scientifica; serve, soprattutto, una *società informata*, consapevole dei rischi e dotata degli strumenti cognitivi per distinguere il vero dal falso[32].

Solo così sarà possibile sfruttare le potenzialità delle tecnologie generative – che aprono prospettive straordinarie nel cinema, nell'arte, nella formazione e nella comunicazione – senza sacrificare sull'altare dell'innovazione la dignità delle persone, la stabilità delle istituzioni e la qualità del discorso democratico[33].

[31] Sul punto si veda G. PESCI, *Educazione civica e cittadinanza digitale*, Milano, 2024.
[32] Sul rapporto con il diritto d'autore si veda R. LANZO, *Influencer e intelligenza artificiale. Dai deepfake ai diritti d'autore sui contenuti creati con l'AI*, Rimini, 2025. Con un approccio più pratico si veda L. TURINI, *A chi spettano i diritti sulle opere dell'intelligenza artificiale*, Rimini, 2024.
[33] Sul tema del futuro dei deepfake si veda Á. FERNÁNDEZ GAMBÍN, A. YAZIDI, A. VASILAKOS, H. HAUGERUD, Y. DJENOURI, *Deepfakes: current and future trends*, in *The Artificial Intelligence Review*, 2024-03, Vol. 57 (3), p. 64.

Profili evolutivi della dimensione esterna del Mercato Unico Digitale

di FEDERICO FERRI*

SOMMARIO: 1. Introduzione. – 2. Accordi riconducibili in via principale alla politica commerciale comune: disposizioni *ad hoc* in accordi di libero scambio. – 3. *Segue*: i nuovi accordi (e partenariati) sul commercio digitale. – 4. Accordi di altra natura: tra commercio, associazione e cooperazione allo sviluppo. – 5. Strumenti diversi dagli accordi: tra intese informali e leve finanziarie. – 6. Ulteriori considerazioni in prospettiva, alla luce della recente Strategia digitale internazionale dell'Unione europea. – 7. Conclusioni.

1. Introduzione

Il Mercato Unico Digitale (MUD) nasce come ambizione "interna" dell'Unione europea (Unione o UE). A partire dalla pubblicazione dell'apposita strategia del 2015 ad opera della Commissione europea[1], il MUD è divenuto il paradigma di riferimento per l'avvio di riforme multisettoriali che, nel loro insieme e in assenza di un'espressa politica in materia nel Trattato sull'Unione europea (TUE) e nel Trattato sul Funzionamento dell'Unione europea (TFUE), hanno dato vita nel tempo a un sistema molto complesso. La complessità del sistema deriva principalmente dalla numerosità dei settori coperti e degli strumenti messi in campo[2], oltre che dagli incroci tra interessi puramente mercantilistici ed

* Ricercatore in Diritto dell'Unione europea, presso *Alma Mater Studiorum* – Università di Bologna, Dipartimento di Scienze giuridiche.

[1] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192, 6.5.2015.

[2] Per contributi che, nel loro insieme, contribuiscono a dare l'idea dell'estensione dell'ambito applicativo del MUD, si veda, senza alcuna pretesa di esaustività, e oltre a quelli contenuti nel presente Numero Speciale: G. CONTALDI (a cura di), *Diritto, mercati e tecnologia* – Fascicolo speciale "*Il mercato unico digitale*", 2018; M. INGLESE, *Regulating the Collaborative Economy in the European Union Digital Single Market*, Cham, 2019; G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Eurojus* – Fascicolo speciale "*Mercato unico digitale, dati personali e diritti fondamentali*", 2020, p. 13 ss.; S. GARBEN, I. GOVAERE (a cura di), The *Internal Market 2.0*, Oxford-New York, 2020; P. MANZINI, G. CONTALDI, G. CAGGIANO (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021; T.-E. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU-MERDI (a cura di), *EU Internet Law in the Digital Single Market*, Cham, 2021; Ł. D. DĄBROWSKI, M. SUSKA (a cura di),

esigenze di tutela dei diritti fondamentali[3]. Con il passare degli anni,

The European Union Digital Single Market: Europe's Digital Transformation, Oxon-New York, 2022; F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Torino, 2022, p. 53 ss.; G. MORGESE, *Moderazione e rimozione dei contenuti illegali online nel diritto dell'UE*, in *Federalismi.it*, 2022, p. 80 ss.; S. LAVAGNINI, *Il diritto d'autore nel mercato unico digitale. Direttiva (UE) 2019/790 e D.lgs. n. 177/2021 di recepimento*, Torino, 2022; L. ARCELIN (dir.), *Les régulations européennes du numérique et le droit du marché*, Bruylant, 2024 ; V. PAPAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU, Act-ification, GDPR Mimesis and EU Law Brutality at Play*, Oxon-New York, 2024; P. VOIGT, N. HULLEN, *The EU AI Act: Answers to Frequently Asked Questions*, Berlin, 2024; C. N. PEHLIVAN, N. FORGÓ, P. VALCKE (a cura di), *The EU Artificial Intelligence (AI) Act: A Commentary*, Alphen aan den Rijn, 2024; B. NASCIMBENE, *Il mercato unico digitale è una nuova frontiera dell'integrazione europea?*, in *Eurojus*, n. 3/2025, p. 110 ss.; L. COTINO HUESO, D. U. GALETTA, *The European Union Artificial Intelligence Act: A Systematic Commentary*, Napoli, 2025; A. HUERGO LORA, G. M. DÍAZ GONZÁLEZ (a cura di), *The EU Regulation on Artificial Intelligence: a Commentary*, Milano, 2025; W. KILIAN, *EU Digital Markets Law. A Concise Guide to the Regulations and Directives on IT and Media Law*, Cheltenham-Northampton, 2025; K. WECKSTRÖM, M. L. MONTAGNANI, K. KLAFKOWSKA-WAŚNIOWSKA (a cura di), *Governance of Digital Single Market Actors*, Cheltenham-Northampton, 2025.

[3] Per spunti analitici che permettano di ricavare una panoramica sugli intrecci tra MUD e diritti fondamentali, si rinvia, ancora una volta a titolo meramente esemplificativo, a: J. L. DA CRUZ VILAÇA, *L'application de la Charte dans l'ère du numérique*, in *Revista de Derecho Comunitario Europeo*, 2020, p. 447 ss.; D. LECZYKIEWICZ, *Judicial Development of EU Fundamental Rights Law in the Digital Era: A Fresh Look at the Concept of 'General Principles*', in U. BERNITZ, X. GROUSSOT, J. PAJU, S. A. DE VRIES (a cura di), *General Principles of EU Law and the EU Digital Order*, Alphen aan den Rijn, 2020, p. 65 ss.; O. POLLICINO (ed.), *Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?*, Oxford, 2021; S. SEUBER, C. BECKER, *The Democratic Impact of Strengthening European Fundamental Rights in the Digital Age: The Example of Privacy Protection,* in *German Law Journal*, 2021, p. 31 ss.; G. DE GREGORIO, *Digital Constitutionalism in Europe. Reframing Rights and Powers in the Algorithmic Society*, Cambridge, 2022; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?,* in *Il Diritto dell'Unione europea* – Osservatorio, 17 marzo 2022, p. 1 ss.; F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo,* in *Il Diritto dell'Unione europea*, 2022, p. 277 ss.; C. SCHEPISI, *Diritti fondamentali, principi democratici e* rule of law*: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale,* in *Studi sull'integrazione europea*, 2022, p. 41 ss.; A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione,* in *I Post di AISDUE*, 14 marzo 2023, p. 321 ss.; C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORNIO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, p. 1 ss.; I. ANRÒ, Online hate speech*: la prospettiva dell'Unione europea tra regolamentazione della condotta dei prestatori di servizi intermediari e ricorso al diritto penale,* in *Osservatorio sulle fonti*, 2023, p. 13 ss.; G. FROSIO, C. GEIGER, *Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime*, in *European Law Journal*, 2023, p. 31 ss.; B. NASCIMBENE, F. ROSSI DAL POZZO,

comunque, il MUD e, più in generale, la transizione digitale, si sono sempre confermati obiettivi apicali dell'Unione. Tuttavia, limitare lo studio del MUD alla sua dimensione interna sarebbe approssimativo: oggi più che mai occorre occuparsi anche della dimensione esterna, certamente meno visibile, ma teoricamente fondamentale.

D'altronde, in un'epoca nella quale vi sono similitudini sempre più pronunciate tra le dimensioni esterna e interna della condizionalità politica UE[4], è noto che l'Unione aspira a utilizzare la transizione digitale come laboratorio per produrre regole in grado di condizionare le condotte di soggetti che orbitano al di fuori di essa: una Unione, insomma, che tenta di agire come *global regulator*[5]. Ciò è alla base di obiettivi di medio e lungo raggio dell'Unione, quali l'affermazione di un'autonomia strategica e di una sovranità tecnologica, divenuti "mantra" ricorrenti nella narrativa UE a seguito dei forti sconvolgimenti geopolitici degli ultimi tempi, come il prolungarsi dell'invasione russa in Ucraina, l'*escalation* dei conflitti che coinvolgono Israele, le interferenze cinesi nell'economia dell'Unione, le guerre commerciali originate dagli Stati Uniti. Pur in assenza di definizioni oggettivamente chiare, e nonostante intuibili difficoltà di applicazione in ambito giuridico, è pacifico che tanto l'autonomia strategica quanto la sovranità tecnologica presuppongono la difesa dei diritti fondamentali e dei valori *ex* art. 2 TUE, nonché la loro vigorosa promozione all'esterno dell'ordinamento giuridico UE, ragion per cui la dottrina si è occupata ampiamente di questi concetti[6].

L'evoluzione dei diritti e delle libertà fondamentali nel settore dei media. Diritto dell'Unione europea, orientamenti giurisprudenziali e recenti interventi normativi, in *Eurojus*, 2023, p. 1 ss.; A. ENGEL, X. GROUSSOT, G. T. PETURSSON (a cura di), *New Directions in Digitalisation. Perspectives from EU Competition Law and the Charter of Fundamental Rights*, Cham, 2025.

[4] A. CIRCOLO, *La condizionalità politica nella dimensione esterna e interna dell'azione dell'Unione europea,* in *Il Diritto dell'Unione europea*, 2022, p. 225 ss.

[5] E. FAHEY, *The EU as a Global Digital Actor. Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022.

[6] In argomento, E. CELESTE, *Digital Sovereignty in the EU: Challenges and Future Perspectives*, in F. FABBRINI E. CELESTE, J. QUINN (a cura di), *Data Protection Beyond Borders. Transatlantic Perspectives on Extraterritoriality and Sovereignty*, Oxford-New York-Dublin, 2021, p. 211 ss.; N. HELWIG, V. SINKKONEN, *Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term*, in *European Foreign Affairs Law Review*, 2022, p. 1 ss.; S. POLI, E. FAHEY, *The Strengthening of the European Technological Sovereignty and its Legal bases in the Treaties*, in *Eurojus*, 2022, p. 147 ss.; H. SHEIKH, *European Digital Sovereignty: A Layered Approach,* in *Digital Society*, 2022, p. 20 ss.; D. BROEDERS, F. CRISTIANO, M. KAMINSKA, *In Search of Digital Sovereignty and Strategic Autonomy: Normative Power*

E allora, sin dai primi orientamenti sul MUD è apparso chiaro che costruire la proiezione esterna di questo spazio sarebbe stato un passaggio successivo e avrebbe implicato il ricorso graduale a quell'area dell'azione esterna che più di qualunque altra si combina con il mercato interno, ovvero la politica commerciale comune (PCC)[7]. Nella comunicazione sul MUD del 2015 si dichiarava che «[u]na volta completato, il Mercato Unico Digitale offrirà alle imprese un ordine di grandezza tale da aiutarle ad espandersi oltre il mercato interno dell'UE e aumenterà ulteriormente l'attrattiva che l'Unione è in grado di esercitare sulle imprese del mondo. Occorre mantenere l'apertura del mercato europeo e svilupparla ulteriormente nella sfera digitale. L'UE dovrebbe continuare a spingere per ottenere dai partner commerciali la stessa apertura […]. In questo senso si dovrebbe lavorare ulteriormente per definire una politica ambiziosa in tema di commercio e investimento nel settore digitale, anche mediante la conclusione di accordi di libero scambio da parte dell'UE»[8].

Successivamente, la Commissione ha ridefinito alcuni contorni del rapporto tra MUD e azione esterna, riferendosi a un modello europeo di fondo in base al quale l'UE «dovrebbe sfruttare il proprio potere regolamentare, le capacità industriali e tecnologiche potenziate, le risorse diplomatiche e gli strumenti di finanziamento esterno per plasmare le interazioni globali»; e in questa cornice sono stati ricompresi anche gli

---

Europe to the Test of Its Geopolitical Ambitions, in *Journal of Common Market Studies*, 2023, p. 1261 ss.; C. BEAUCILLON, S. POLI (a cura di), *European Papers* – Numero Speciale, "*EU Strategic Autonomy and Technological Sovereignty: An Introduction*", 2023; J. CARVER, *More Bark than Bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy*, *in* Journal of European Public Policy, 2023, p. 2250 ss.; P. DE PASQUALE, F. FERRARO, *L'autonomia strategica dell'Unione europea: dalla difesa…alla politica commerciale c'è ancora tanta strada da fare*, in *Diritto pubblico comparato ed europeo*, n. 2/2023, p. V ss.; A. MIGLIO, G. PEROTTO, L. GROSSIO, *I meccanismi di finanziamento del settore difesa nell'Unione europea e il loro contributo al rafforzamento dell'autonomia strategica* (Centro Studi sul Federalismo, 2024, p. 9 ss.): S. POLI, D. GALLO, *Enhancing European Technological Sovereignty: The Foreign Investment Screening Regulation and Beyond*, in K. A. ARMSTRONG, J. SCOTT, J. THEIS (a cura di), *EU External Relations And The Power of Law*: Liber Amicorum *in Honour of Marise Cremona*, Oxford, 2024, p. 215 ss.

[7] È pacifico che l'esistenza della PCC sia stata legata al mercato interno sin dalle origini del processo di integrazione europea: cfr. anche R. ADAM, A. TIZZANO, *Manuale di Diritto dell'Unione europea*, Torino, 2014, p. 839. Si è comunque fatto presente che la PCC non è soltanto la «*external face*» del mercato interno, dal momento che essa persegue obiettivi di una più vasta agenda esterna e si lega anche ad altri strumenti e politiche: in questo senso, M. CREMONA, *The Internal Market and the External Economic Relations,* in P. KOUTRAKOS, J. SNELL (a cura di), *Research Handbook on the Law of the EU's Internal Market*, Cheltenham-Northampton, 2017, p. 479 ss.

[8] COM(2015) 192 final, cit., p. 20.

accordi commerciali e di associazione[9].

Tale proposito è stato sviluppato anche in iniziative relative alla PCC. Già il Parlamento europeo, all'indomani della pandemia di COVID-19, aveva sottolineato la necessità di agevolare i tentativi di ripresa internazionali facendo perno su un commercio aperto ed equo e riferendosi anche al commercio digitale[10]. La strategia della Commissione di riesame della PCC[11] è andata oltre, confermando l'avvenuto avvio del passaggio preconizzato nel 2015, che, come si può intuire, trascende i limiti della nota teoria del *Brussels effect*[12]. Nel documento si è annunciata la centralità, tra gli obiettivi della PCC, di una trasformazione dell'economia UE in linea con la trasformazione digitale. Detto obiettivo – si è scritto – deve essere raggiunto diversificando le relazioni e costruendo alleanze con *partners* che condividono gli stessi principi, anche attraverso l'ampia rete di accordi commerciali, con un'enfasi particolare sugli accordi di libero scambio (ALS). Risultavano invece più tenui i riferimenti agli strumenti della politica esterna di sviluppo e di assistenza dell'UE[13], come gli accordi di partenariato economico (APE).

Alla luce di questi cenni introduttivi, pare allora di interesse comprendere quali siano state le principali coordinate delle iniziative giuridiche che hanno scandito l'evoluzione della dimensione esterna del MUD fino ad oggi, e ragionare su possibili implicazioni di diritto sovranazionale. Ci si interroga soprattutto sulle tipologie di strumenti e competenze e sulla portata degli obblighi o impegni più caratterizzanti. Le relazioni considerate sono quelle che legano direttamente l'Unione a Stati terzi, con precipuo riferimento a paesi che non rientrano nel gruppo dei candidati all'adesione o nell'area del vicinato UE. Per ragioni di ordine e spazio non si indugerà su singoli strumenti minori attinenti a specifiche

---

[9] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final, 19.2.2020, pp. 13-14.

[10] Risoluzione del Parlamento europeo del 7 ottobre 2020 sull'attuazione della politica commerciale comune - relazione annuale 2018 (2019/2197(INI)), punto 74.

[11] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Riesame della politica commerciale - Una politica commerciale aperta, sostenibile e assertiva*, COM(2021) 66 final, 18.2.2021.

[12] A. BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

[13] V. anche Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale, *Un mercato unico digitale connesso per tutti*, COM(2017) 228 final,10.5.2017, p. 27.

aree materiali del MUD, prediligendo invece elementi di prassi che consentano di trarre spunti di più ampio respiro.

L'analisi che si intende compiere si dipana come segue. L'attenzione viene diretta dapprima verso varie categorie di accordi internazionali conclusi dall'Unione in epoca recente: da un lato, quelli più propri della PCC, come gli ALS (par. 2) e i nuovi accordi sul commercio digitale (par. 3); dall'altro, accordi di natura più complessa, nei quali la componente di libero scambio interseca esigenze di carattere assistenziale (par. 4). Seguono considerazioni su ulteriori forme di cooperazione che esulano dalla sfera degli accordi e si sostanziano in intese informali o soluzioni finanziarie, con *focus* sul continente africano (par. 5). Quindi, ci si propone di affacciarsi al tema d'indagine anche in chiave prospettica, cioè dall'angolo di visuale della recente Strategia digitale internazionale per l'Unione europea (par. 6). Da ultimo, si presentano le conclusioni del lavoro (par. 7).

2. Accordi riconducibili in via principale alla politica commerciale comune: disposizioni *ad hoc* in accordi di libero scambio

La prima strada da battere è quella che porta alla politica commerciale comune dell'Unione europea, la quale, come noto, segue le regole dell'art. 207 TFUE ed è governata dai principi dell'art. 21 TUE[14]. Questa politica,

[14] Per approfondimenti sulla PCC e sulla rispettiva evoluzione si veda: P. EECKHOUT, *EU External Relations Law*, Oxford, 2011, p. 439 ss.; M. KRAJEWSKI, *The Reform of the Common Commercial Policy*, in A. BIONDI, P. EECKHOUT, S. RIPLEY (a cura di), *EU Law after Lisbon*, Oxford, 2012, p. 292 ss.; A. CALIGIURI, *Art. 207 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Milano, 2014, p. 1706 ss.; P. KOUTRAKOS, *EU International Relations Law*, Oxford-Portland, 2015, p. 17 ss.; C. KADDOUS, *The Transformation of the EU Common Commercial Policy,* in P. EECKHOUT, M. LOPEZ-ESCUDERO (a cura di), *The European Union's External Action in Times of Crisis,* Oxford-Portland, 2016, p. 429 ss.; M. CREMONA, *The Principle of Conferral and Express and Implied External Competences,* in E. NEFRAMI, M. GATTI (a cura di), *Constitutional Issues of EU External Relations Law*, Baden-Baden, 2018, p. 33 ss. ; M. BUNGENBERG, C. HERRMANN, *Common Commercial Policy after Lisbon*, Heidelberg, 2013; F. ERLBACHER, T. M. RUSCHE, *Articles 206-207*, in M. KELLERBAUER, M. KLAMERT, J. TOMKIN (a cura di), *The EU Treaties and the Charter of Fundamental Rights: A Commentary*, Oxford, 2019, p. 1585 ss.; M. HAHN, G. VAN DER LOO (a cura di), *Law and practice of the Common Commercial Policy: the first 10 years after the Treaty of Lisbon*, Leiden, 2020; J. LARIK, *Common Commercial Policy*, in R. A. WESSEL, J. LARIK (a cura di), *EU External Relations Law: Text, Cases and Materials*, Oxford, 2020, p. 209 ss.; F. MARTINES, *La politica commerciale comune*, in R. TORINO, C. DI MAIO (a cura di), *Diritto e politiche dell'Unione europea*, Milano-Padova, 2020, p. 241; P. MUSQUAR, *Politique commerciale de l'Union européenne*, Buxelles, 2020; F. BESTAGNO, *La Politica commerciale comune*, in M. E. BARTOLONI, S. POLI (a cura di), *L'azione esterna*

che ricomprende atti sostanzialmente destinati a promuovere, facilitare o disciplinare gli scambi internazionali (e che sortiscono su di essi effetti diretti e immediati)[15] funge teoricamente da ambito privilegiato di sperimentazione e affermazione delle traiettorie giuridiche esterne del Mercato Unico Digitale. Il punto è capire se tali direttrici trovano espressione negli strumenti più tradizionali, vale a dire all'interno di accordi commerciali, oppure altrove.

Fatte queste premesse, si ricorda che è da circa un ventennio che l'Unione europea lavora alla costruzione di ALS ampi e ambiziosi dal punto di vista del campo di applicazione, tant'è vero che gli accordi di questo genere conclusi nell'epoca *post*-Lisbona vengono denominati "di nuova generazione"[16]. La *ratio* dell'estensione tematica dei nuovi ALS risiede nell'esigenza di stringere relazioni commerciali più produttive con *partners* che si collocano ben al di là della sfera della politica di vicinato UE.

Se il ricorso a tale categoria di strumenti si è intensificato per ragioni facilmente intuibili, non si deve dimenticare come l'Unione abbia mantenuto un orientamento tutto sommato prudente. Indicative sono le parole della Commissione europea in una comunicazione nella quale si esploravano nuove vie esterne per rafforzare la crescita e l'occupazione nell'Unione[17]. Nel documento viene precisato che gli ALS di futura definizione avrebbero potuto muovere dai principi del diritto dell'Organizzazione Mondiale del Commercio (OMC) e dalle altre regole pertinenti di diritto internazionale, ma a patto che ciò fosse gestito «con attenzione»; l'intento era di prevedere una liberalizzazione pressoché

---

dell'Unione europea, Napoli, 2021, p. 111 ss.; J. WOUTERS, F. HOFFMEISTER, G. DE BAERE, T. RAMOPOULOS (a cura di), *The Law of EU External Relations: Cases, Materials, and Commentary on the EU as an International Legal Actor* (3rd edn), Oxford, 2021, p. 230 ss.; M. CREMONA, J. KUKAVICA, *Common Commercial Policy and the Determination of Exclusivity: Opinion 1/75 (Local Cost Standard)*, in G. BUTLER, R. A. WESSEL (a cura di), *EU External Relations Law: The Cases in Context*, Oxford, 2022, p. 45 ss.

[15] V., ad esempio, Corte giust., 16 maggio 2015, parere 2/15, *Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore*, ECLI:EU:C:2017:376, punto 36; Corte giust., 18 luglio 2013, causa C-414/11, *Daiichi Sankyo*, ECLI:EU:C:2013:520, punto 51; Corte giust., 22 ottobre 2013, causa C-137/12, *Commissione c. Consiglio*, ECLI:EU:C:2013:675, punto 57.

[16] Cfr, in particolare G. ADINOLFI (a cura di), *Gli accordi preferenziali di nuova generazione dell'Unione europea*, Torino, 2021.

[17] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Europa Globale: Competere Nel Mondo. Un contributo alla strategia per la crescita e l'occupazione dell'UE,* COM(2006) 567, 4.10.2006, pp. 9-10.

generalizzata degli scambi, andando così oltre i confini delle discipline dell'OMC, anche per scongiurare i rischi potenziali che ALS particolarmente ristretti avrebbero potuto arrecare al sistema multilaterale di scambi. Si caldeggiava allora una selezione dei *partners* sulla base di due criteri economici di fondo: il potenziale di mercato e il livello di protezione contro gli interessi dell'UE in materia di esportazioni.

È in questo mutato contesto – per larghi tratti sovrapposto all'espansione della digitalizzazione quale fattore di spinta nel commercio internazionale[18] – che l'UE ha elaborato i primi modelli di regole applicabili all'odierno commercio digitale, anche se in ritardo rispetto alle azioni di analogo tenore intraprese da vari Stati terzi[19]. Si tratta dei capitoli sul "commercio elettronico", che figurano anzitutto negli ALS UE-Corea del Sud[20] (artt. 7.48-7.49) e UE-Vietnam[21] (artt. 8.50-8.52). Considerazioni del tutto similari valgono per certi accordi di associazione volti a istituire le cosiddette "*Deep And Comprehnsive Free Trade Areas*", cioè quelli con Ucraina[22] (Artt. 139-140), Georgia[23] (artt. 127-128) e Moldova (artt. 254-255)[24]. Quei capitoli si ritrovano con la stessa denominazione, ma in forma leggermente più sviluppata, negli ALS – meno risalenti – che l'UE ha concluso con il Canada[25] (Capitolo 16) e con Singapore[26] (Artt. 8.57-8.61).

Sostanzialmente, nei capitoli sul commercio elettronico le parti hanno convenuto il divieto di applicare dazi alle trasmissioni elettroniche; per il

---

[18] V. M. BURRI, *The Impact of Digitalization on Global Trade Law,* in *German Law Journal*, 2023, p. 551 ss.

[19] Così M. BURRI, *Digital Trade Rulemaking in Free Trade Agreements*, in D. COLLINS, M. GEIST (a cura di) *Handbook on Digital Trade*, Cheltenham, 2023, p. 22.

[20] Accordo di libero scambio tra l'Unione europea e i suoi Stati membri, da una parte, e la Repubblica di Corea, dall'altra, in GUUE del 14 maggio 2011, L 127/6.

[21] Accordo di libero scambio tra l'Unione europea e la Repubblica socialista del Vietnam, in GUUE del 12 giugno 2020, L 186/3.

[22] Accordo di associazione tra l'Unione europea e la Comunità europea dell'energia atomica e i loro Stati membri, da una parte, e l'Ucraina, dall'altra, in GUUE del 29 maggio 2014, L 161/3.

[23] Accordo di associazione tra l'Unione europea e la Comunità europea dell'energia atomica e i loro Stati membri, da una parte, e la Georgia, dall'altra, in GUUE del 30 agosto 2014, L 261/4.

[24] Accordo di associazione tra l'Unione europea e la Comunità europea dell'energia atomica e i loro Stati membri, da una parte, e la Moldova, dall'altra, in GUUE del 30 agosto 2014, L 260/4.

[25] Accordo economico e commerciale globale (CETA) tra il Canada, da una parte, e l'Unione europea e i suoi Stati membri, dall'altra, in GUUE 14 gennaio 2017, L 11/23.

[26] Accordo di libero scambio tra l'Unione europea e la Repubblica di Singapore, in GUUE 14 novembre 2019, L 294/3.

resto, il tema viene affidato alla copertura delle regole OMC. Tutt'al più, si prende atto dell'importanza del commercio elettronico per gli scambi commerciali (in alcuni casi anche per lo sviluppo sociale[27]) e si stabiliscono elenchi abbastanza limitati di priorità di dialogo per favorire una cooperazione più strutturata tra le parti. Ne deriva che le fondamenta giuridiche delle relazioni commerciali intrattenute dall'Unione con i *partners* suddetti lasciano ampio margine di azione alle parti e fanno sì che le iniziative individuali riconducibili a tali accordi possano facilmente sottrarsi al raggio d'azione dei meccanismi giurisdizionali di risoluzione delle controversie di volta in volta previsti. Il tutto senza dimenticare che questi gruppi di norme, essendo riferiti principalmente ai mezzi di trasmissione di beni e servizi, mal si adattano al passaggio dall'analogico al digitale che fa da sfondo all'emersione del MUD.

Con il passare del tempo, si è assistito a un progressivo cambio di passo, segnato anche dalla scelta semantica di utilizzare l'espressione "commercio digitale" in luogo di "commercio elettronico". Tenendo presente che, pur essendo formule simili, la seconda pare essere più estesa della prima[28], non sfugge come in vari ALS firmati di recente la disciplina in materia risulti più elaborata[29]. Ci si riferisce, in specie, ai capitoli sul commercio digitale contenuti negli ASL conclusi dall'UE con Messico[30] (Capitolo 16), Cile[31] (Capitolo 19) e Nuova Zelanda[32] (Capitolo 12). L'accordo di partenariato economico tra UE e Giappone[33] (Artt. 8.70-8.81) sembra a prima vista collocarsi a metà strada tra le due fasi che si stanno illustrando, ma va letto alla luce di un apposito protocollo di modifica che

[27] Es. ALS UE-Canada, Art. 16.4.

[28] J.A. MICALLEF, *Digital Trade in EU FTAs: Are EU FTAs Allowing Cross Border Digital Trade to Reach Its Full Potential?,* in *Journal of World Trade*, p. 855 ss.; W. ALSCHNER, *E-commerce or Digital Trade? Why the Difference Should Matter to Trade Lawyers*, in D. COLLINS, M. GEIST (a cura di)*, op cit.*, p. 54 ss.

[29] V. REMONDINO, *Gli accordi sul commercio digitale tra liberalizzazione degli scambi e protezione dei dati personali e della privacy: implicazioni per la politica commerciale comune dell'Unione europea*, in *Quaderni AISDUE*, n. 2/2024, p. 204 ss.

[30] L'accordo di principio è consultabile al seguente indirizzo *Internet*: https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/mexico/eu-mexico-agreement/text-agreement_en, dove è possibile reperire anche le proposte della Commissione europea su firma e conclusione dell'accordo globale aggiornato UE-Messico.

[31] Accordo interinale sugli scambi tra l'Unione Europea e la Repubblica del Cile, in GUUE del 20 dicembre 2024, L 149/1.

[32] Accordo di Libero Scambio tra l'Unione Europea e la Nuova Zelanda, in GUUE del 25 marzo 2024, L 2024/866.

[33] Accordo tra l'Unione europea e il Giappone per un partenariato economico, in GUUE del 27 dicembre 2018, L 330/3.

completa soprattutto le regole su dati personali e *privacy*[34]. L'accordo sugli scambi commerciali e la cooperazione con il Regno Unito[35] (TCA UE-UK, Artt. 196-212) propone un impianto regolatorio più ricco in relazione al commercio digitale.

Vi sono certamente delle similitudini nei contenuti dei capitoli sul commercio digitale che figurano in questi strumenti[36], poiché già in sede di negoziato è previsto che il "blocco europeo" proponga alla controparte una matrice preimpostata. Questi capitoli si aprono solitamente con regole generali in punto di obiettivi, ambito di applicazione e definizioni principali. Seguono disposizioni concernenti, a vario titolo, il diritto di ciascuna parte di legiferare nei propri territori per il conseguimento di obiettivi legittimi (*right to regulate*) e il divieto di autorizzazioni preventive circa la prestazione di un servizio per via elettronica. Il fulcro dei capitoli sul commercio digitale rimane il divieto di applicare dazi doganali sulle trasmissioni elettroniche. A ciò adesso si aggiungono regole rientranti in una clausola a vocazione orizzontale non negoziabile[37] e volta a garantire i flussi di dati transfrontalieri senza minare la localizzazione degli stessi; accanto a questi obblighi spiccano prescrizioni sulla tutela dei dati personali e della *privacy*. Non mancano accorgimenti per assicurare la tutela (in talune ipotesi, la fiducia) dei consumatori *online*. Si segnalano anche disposizioni su settori specifici, come la conclusione di contratti per via elettronica, le firme elettroniche e la protezione del codice sorgente del *software.* Sono poi previsti impegni di cooperazione e dialogo normativo su priorità che variano da strumento a strumento.

Una simile costruzione si ritrova anche nei documenti che preludono ai capitoli sul commercio digitale di ALS non ancora firmati, ma giunti a uno stadio negoziale quantomeno avanzato, come quelli tra Unione e,

---

[34] Protocollo che modifica l'Accordo tra l'Unione europea e il Giappone per un partenariato economico, in GUUE del 14 maggio 2024, L 2024/1304.

[35] Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, in GUUE del 30 aprile 2021, L 149/10.

[36] Un caso a sé stante è il TCA UE-UK, che fa menzione del commercio digitale già nel preambolo. Al punto 11 le parti dichiarano di riconoscere l'importanza di agevolare nuove opportunità per le imprese e i consumatori con il commercio digitale e di voler eliminare «gli inutili ostacoli al flusso di dati e agli scambi per via elettronica, nel rispetto delle norme delle parti sulla protezione dei dati personali».

[37] https://ec.europa.eu/newsroom/just/items/627665/en. V. *amplius* S. YAKOVLEVA, K. IRION, *Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade*, in *International Data Privacy Law*, 2020, p. 201 ss.

nell'ordine, Australia[38], Emirati Arabi Uniti[39], India[40], Indonesia[41] (a differenza di quanto sta avvenendo nei lavori preparatori dell'accordo UE-Mercosur[42]).

Nonostante il consolidamento del rinnovato e più incisivo approccio UE al commercio digitale negli ALS[43], si ritiene tuttavia che permangano ancora varie questioni giuridiche controverse, le quali concorrono a riprodurre un quadro d'insieme piuttosto nebuloso.

In primis, è evidente che i capitoli di cui trattasi sono il frutto di un compromesso tra soggetti teoricamente alla pari dal punto di vista dei rapporti di forza intesi in senso lato. Dunque, è difficile immaginarsi l'inclusione, (anche) in questi capitoli, di previsioni idonee a circoscrivere in misura significativa le future scelte dei decisori politici delle parti coinvolte.

Parimenti, non vi è da stupirsi se le disposizioni di riferimento non rispecchiano realmente la generale evoluzione del MUD. O meglio, benché non siano mancati aggiornamenti tematici, si è ben lontani dall'avere una piena corrispondenza tra l'intensa produzione normativa

---

[38] Per maggiori informazioni, si veda il seguente indirizzo *Internet* https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/australia/eu-australia-agreement_en.

[39] Per maggiori informazioni, si veda il seguente indirizzo *Internet* https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/gulf-region/eu-united-arab-emirates-agreement/eu-united-arab-emirates-documents_en. Si segnala che il Capitolo 11 copre anche il tema degli *open governance data*, analogamente a quanto previsto nel TCA UE-UK.

[40] Per maggiori informazioni, si veda il seguente indirizzo *Internet* https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/india/eu-india-agreements/documents_en. Anche in questo caso, si enfatizza il *focus* sugli *open government data*.

[41] Per maggiori informazioni, si veda il seguente indirizzo *Internet* https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/indonesia/eu-indonesia-agreement/documents_en. Un elemento di potenziale novità è l'inclusione di disposizioni dedicate agli appalti pubblici nel Capitolo "*Digital Trade*". Rileva altresì che sono state avviate discussioni approfondite sulle eccezioni relative alla sicurezza (Report of the Twelfth Round of Negotiations on a Free Trade Agreement between the European Union and India - 7-11 July 2025).

[42] Proposta di decisione del Consiglio relativa alla conclusione, a nome dell'Unione europea, dell'accordo di partenariato tra l'Unione europea e i suoi Stati membri, da una parte, e il Mercato comune del Sud, la Repubblica argentina, la Repubblica federativa del Brasile, la Repubblica del Paraguay e la Repubblica orientale dell'Uruguay, dall'altra, COM(2025) 397 final, 3.9.2025 (che contiene previsioni più limitate e organizzate in maniera diversa: v. soprattutto artt. 6.5 e 8.10).

[43] V., ad esempio, M. BURRI, K. KUGLER, A.D. KER, *Digital Trade in the EU–New Zealand Free Trade Agreement: An Appraisal*, in *Legal Issues of Economic Integration*, 2024, p. 11 ss.

interna derivante dai numerosissimi atti legislativi dell'Unione (molti dei quali di armonizzazione, ancorché con gradazioni variabili) e la copertura complessiva delle regole contenute nei capitoli sul commercio digitale. Si può sostenere che negli ALS considerati sinora vi sia tutt'al più qualche coordinata orientativa, una serie abbastanza ristretta di principi guida ispirati a una "politica" interna molto più densa e articolata. Quanto sostenuto vale anche in relazione alla dimensione assiologica che il MUD ha via via acquisito e che nei capitoli sul commercio digitale appare molto più sfumata.

Per quanto difficile da colmare mediante strumenti come gli ALS, questo ampio divario è suscettibile di dare luogo a problematiche, anche in rapporto a importanti questioni di natura costituzionale, come la tutela dei diritti fondamentali. Vale la pena citare un esempio lampante, riconducibile al TCA UE-UK. Sebbene questo accordo leghi l'Unione a uno Stato terzo che ha una forte familiarità con il diritto UE, nel caso di specie è stata addirittura lamentata una *deminutio* della clausola orizzontale non negoziabile su flussi transfrontalieri e protezione dei dati, al punto che si è dichiarato che «the wording agreed with the UK on data protection and privacy must remain an exception»[44].

Un ulteriore elemento che traspare da un confronto tra i testi di questi strumenti è la sussistenza di differenze tra più definizioni ed espressioni. Ancora una volta, i profili di disomogeneità riguardano anche disposizioni centrali dei capitoli sul commercio digitale, ossia quelle della predetta clausola orizzontale e non negoziabile sugli obblighi da assumere in materia di dati. Ora, se è vero che il ricorso a parole differenti talvolta può comunque condurre l'interprete all'individuazione della medesima risultanza concettuale, non si può al contempo escludere che a formulazioni distinte corrispondano conseguenze giuridiche di diverso tenore a seconda dell'accordo preso in esame[45].

Ma questo mosaico a più coloriture pare in realtà sovrastare una superficie più ampia di quella riferibile al tema definitorio. Come notato in dottrina, e al netto di una maggiore uniformità rispetto al passato, ciò

[44] Ci si riferisce alla posizione del Garante europeo della protezione dei dati, con la quale tale criticità è stata sottolineata vigorosamente (EDPS *Opinion 3/2021 on the Conclusion of the EU and UK Trade Agreement and the EU and UK Exchange of Classified Information Agreement*, 22 febbraio 2021, disponibile a questo indirizzo *Internet*: https://www.edps.europa.eu/system/files/2021-02/2021_02_22_opinion_eu_uk_tca_en.pdf , spec. punto 21).

[45] In tal senso, M. BURRI, K. KUGLER, *Regulatory Autonomy in Digital Trade Agreements,* in *Journal of International Economic Law*, 2024, p. 402.

che a lungo si è stagliato agli occhi dell'interprete è pur sempre «a rule-making landscape characterized by considerable diversity depending on the timing of agreements and the nature (and development level) of the Union's trading partners»[46]. È quindi lecito immaginare il prodursi di specifici micro-regimi giuridici, che andrebbero ad aggiungersi allo scenario a geometria tendenzialmente variabile prodotto sinora dall'evoluzione del MUD a livello interno[47].

Va altresì detto che il campo di applicazione di questo o quel capitolo sul commercio digitale rischia di risentire dell'effetto di una gamma mutevole di esenzioni ed eccezioni, in considerazione dello specifico ALS. Oltretutto, le disposizioni che affermano il *right to regulate*, tipiche degli ALS conclusi dall'Unione e mutuate dalla struttura dei trattati sugli investimenti, si estendono ad una nutrita casistica di ipotesi, peraltro passibile di ulteriore ampliamento, a testimonianza del fatto che le parti sembrano godere di una certa libertà nell'identificazione dell'interesse pubblico da perseguire e nell'attuazione di restrizioni interne giustificabili in tal senso[48].

3. *Segue*: i nuovi accordi (e partenariati) sul commercio digitale

Negli ultimi anni l'Unione europea ha iniziato a sviluppare un approccio più organico al tema del commercio digitale nelle relazioni che coinvolgono gli Stati terzi con cui ha concluso ALS. Con alcuni di essi, infatti, si è dato vita a nuovi strumenti che riguardano espressamente il commercio digitale. Questo modello è ancora in fase embrionale e riprende in parte la struttura dell'Accordo OMC sul commercio elettronico[49].

---

[46] P. SAUVÉ, M. SOPRANA, *The Evolution of the EU Digital Trade Policy,* in M. HAHN, G. VAN DER LOO (a cura di), *op. cit*., p. 302.

[47] Considerazioni in questo senso sono rinvenibili in più passaggi del recente Rapporto *The Future of European Competitiveness*, redatto da Mario Draghi e pubblicato nel settembre 2024 (https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en).

[48] La questione si situa in un contesto particolarmente complesso anche in ambito OMC: al riguardo, si veda A.D. MITCHELL, *The Right to Regulate and the Interpretation of the WTO Agreement,* in *Journal of International Economic Law*, 2023, p. 462 ss.

[49] Il testo è contenuto in una Dichiarazione congiunta di Australia, Giappone e Singapore, del 26 luglio 2024, ed è disponibile al seguente indirizzo *Internet*: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True. Per commenti sull'iniziativa, cfr. M. BURRI, *A WTO Agreement on Electronic Commerce: An Inquiry Into Its Legal Substance and Viability,* in *Georgetown Journal of International Law*, 2023, p. 565 ss.; A. D. MITCHELL, E. CHIN, *The WTO Joint Statement Initiative on E-commerce: Navigating Digital Trade Rules in a Fragmented World,* in *Journal of World Trade*, 2023, p. 971 ss.

Tuttavia, da un'analisi dei principali elementi innovativi emersi sinora si possono trarre utili spunti di riflessione. Gli strumenti in discorso possono essere suddivisi in due categorie principali, al contempo accomunate da evidenti similitudini e separate da marcate differenze.

La prima categoria racchiude i partenariati digitali che l'Unione ha firmato con quattro Stati terzi allineati tra il 2022 e il 2023: Canada[50], Corea del Sud[51], Giappone[52] e Singapore[53].

Queste *digital partnerships* favoriscono indubbiamente la ramificazione delle relazioni tra parti in molteplici nicchie della transizione digitale. A riprova di quanto si era sostenuto in precedenza, quando ci si riferiva alla ristrettezza dell'ambito di applicazione dei capitoli in materia di commercio digitale degli FTA di ultima generazione conclusi dall'Unione, i quattro partenariati digitali hanno un raggio d'azione molto più ampio. Già la denominazione degli strumenti dovrebbe fare presagire un'estensione tematica, poiché il riferimento non è al commercio digitale, bensì al digitale nel suo insieme. E allora, ecco che i nuovi partenariati si estendono a priorità d'intervento più o meno comuni quali intelligenza artificiale, cybersicurezza, connettività internazionale, 5G/6G, tecnologie quantistiche, tecnologie del linguaggio, semiconduttori, identità digitale, trasformazione digitale delle PMI, *digital skills*. Al centro del progetto figura comunque una visione antropocentrica della transizione digitale.

Va precisato che, sulla scia di un processo di incalzante informalizzazione degli strumenti alla base delle relazioni internazionali alimentato anche dall'Unione e dagli Stati membri[54], i partenariati digitali non sono stati concepiti dalle parti come strumenti vincolanti, e non sono

---

[50] Il testo del partenariato digitale tra UE e Canada è disponibile al seguente indirizzo *Internet*: https://digital-strategy.ec.europa.eu/en/news/canada-european-union-digital-partnership.

[51] Il testo del partenariato digitale tra UE e Corea del Sud è disponibile al seguente indirizzo *Internet*: https://digital-strategy.ec.europa.eu/en/library/republic-korea-european-union-digital-partnership.

[52] Il testo del partenariato digitale tra UE e Giappone è disponibile al seguente indirizzo *Internet*:
https://www.consilium.europa.eu/media/56091/%E6%9C%80%E7%B5%82%E7%89%88-jp-eu-digital-partnership-clean-final-docx.pdf.

[53] Il testo del partenariato digitale tra UE e Singapore è disponibile al seguente indirizzo *Internet*: https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership.

[54] V. più diffusamente A. OTT, *Informalization of EU Bilateral Instruments: Categorization, Contestation, and Challenges,* in *Yearbook of European Law*, 2020, p. 569 ss.

tantomeno suscettibili di determinare implicazioni finanziarie[55]. Essi esprimono l'intenzione di rinsaldare una cooperazione più estesa e aperta a temi che restano inevitabilmente in continuo divenire, e possono eventualmente svolgere una funzione integrativa rispetto agli ALS che vincolano le medesime parti[56]. A questo proposito, è emblematica la spiegazione offerta al punto 12 del partenariato UE-Singapore, ove si afferma che «[g]iven the diversity of issues to be addressed, the Digital Partnership will adopt a flexible and living architecture that supports a range of cooperation modalities».

Tale approccio è corroborato da un sistema di *governance* a schema sostanzialmente libero, nel senso che le parti hanno optato per monitorare l'evoluzione dei partenariati di anno in anno, affidando competenze non meglio specificate a un organo comunemente denominato "Digital Partnership Council"[57].

La seconda categoria, conseguente alla prima, è quella degli Accordi sul Commercio Digitale (ACD). Gli ACD che l'Unione europea al

[55] A scanso di equivoci, nel partenariato digitale UE-Corea del Sud si è pattuito che «[a]ny differences arising from the interpretation or application of the Digital Partnership should be resolved promptly and amicably through consultations between the sides and should not be referred to any national or international tribunal or third party for settlement» (punto 44).

[56] Si è scritto che, così facendo, l'Unione ha impostato le relazioni bilaterali in materia secondo un approccio «*double face*» che attinge al paradigma dell'autonomia strategica aperta: in altre parole, l'UE intende proteggere e promuovere i valori sovranazionali nelle proprie strategie commerciali tramite un costante dialogo con i partner, ma prediligendo un'impostazione morbida – più che coercitiva – e orientata a stimolare un'intensa cooperazione internazionale sul piano normativo: S. VILLANI, *La via europea dell'IA nello scenario internazionale*, in S. POLI, S. MARINAI (a cura di), *L'Unione europea sulla scena internazionale: sfide e trasformazioni sul piano interno ed esterno. Atti del VI Convegno Nazionale AISDUE Università di Pisa, 25-26 ottobre 2024*, Napoli, 2025, p. 325.

[57] Solo il partenariato UE-Corea del Sud offre qualche elemento più dettagliato in merito. Qui il *Digital Partnership Council* viene indirettamente proposto come un tassello importante per l'acquisizione di una forte *leadership* per una *governance* effettiva, si precisa che la presidenza è condivisa tra il Commissario UE per il mercato interno e il Ministro coreano per la Scienza e le tecnologie dell'informazione e della comunicazione, e si indica la principale funzione dell'organo, corrispondente alla preparazione di appositi *deliverables*. Si ritiene che, nell'ambito del partenariato UE-Corea del Sud, l'impegno più tangibile che le parti hanno assunto sia riconducibile alle prerogative del *Digital Partnership Council,* in quanto si rappresenta che esso «should be provided with clear progress reports by its secretariat in order to take stock of the progress achieved and provide strategic guidance on the priorities and next steps» (punto 34).

momento ha definito sono due, quello con la Corea del Sud[58] e quello con Singapore[59]. L'esperienza che sta maturando a livello UE prende dunque le mosse da rapporti ormai consolidati mediante ALS, come illustrato nel paragrafo precedente e dai partenariati digitali definiti recentemente. Occorre aggiungere che anche la Corea del Sud e Singapore sono legati tra loro da un accordo simile, rinominato *Digital Partnership Agreement* (KSDPA)[60] ed entrato in vigore all'inizio del 2023. Ciò significa che entrambi gli ACD di cui è ora parte l'Unione non costituiscono una novità in senso assoluto nel panorama internazionale, nonostante gli esempi sul punto (i cosiddetti *Digital Economy Agreements*) siano ancora poco numerosi[61]. Ne consegue che entrambi gli ACD non rappresentano il portato di un'idea pionieristica, ma sono stati realizzati su una base che tutte le rispettive parti stavano già consolidando da tempo[62].

Preliminarmente, preme specificare che gli ACD con Corea del Sud e Singapore, pur avendo un ambito applicativo giocoforza più ristretto rispetto agli ALS, sono certamente strumenti ascrivibili alla PCC: lo si ricava dalla prassi istituzionale UE, in particolare dalla raccomandazione che la Commissione ha pubblicato per stimolare l'avvio dei negoziati[63] e,

---

[58] Agreement on digital trade Between the European Union and the Republic of Singaporei cui negoziati si sono conclusi il 10 marzo 2025 (in attesa della firma, il testo è disponibile al seguente indirizzo *Internet* https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/1bddb97a-c02e-41e6-95d1-6e41029c880f/details?download=true).

[59] Agreement on digital trade Between the European Union and the Republic of Singapore, firmato il 7 maggio 2025 (il testo è disponibile al seguente indirizzo *Internet* (https://circabc.europa.eu/ui/group/09242a36-a438-40fd-a7af-fe32e36cbd0e/library/66ccfa9f-e239-4893-8e12-64f8ff1d1221/details).

[60] Digital Partnership Agreement Between the Government of the Republic of Korea and the Government of the Republic of Singapore (il testo è disponibile al seguente indirizzo *Internet* https://depository.asean-deal.org/agreement-docs/Korea_Singapore_DEA_full_text_of_agreement.pdf). Benchè lo strumento non sia qualificato come "*agreement*", si tratta certamente di un accordo internazionale, come indica il carattere obbligatorio di numerose disposizioni.

[61] Si rinvia alla recente ricognizione proposta in M. BURRI, M. VÁSQUEZ CALLO-MÜLLER, K. KUGLER, *The Evolution of Digital Trade Law: Insights from TAPED,* in *World Trade Review*, 2024, p. 190 ss., spec. p. 202.

[62] Si segnala l'opinione di chi ritiene che, a seguito di un'analisi dei principali accordi sul commercio digitale a livello mondiale conclusi negli ultimi anni, diverse novità derivino dall'attività di Singapore, al punto da concludere che sia in atto una parziale attenuazione del precedente modello a guida statunitense. Si veda E. JONES, B. KIRA, R., TAVENGERWEI, *Norm Entrepreneurship in Digital Trade: The Singapore-led Wave of Digital Trade Agreements,* in *World Trade Review*, 2024, p. 208 ss.

[63] Commissione europea, Raccomandazione di Decisione del Consiglio che autorizza l'avvio di negoziati per le discipline del commercio digitale con la Repubblica di Corea e

soprattutto, dalla successiva decisione adottata dal Consiglio, che reca quale unica base giuridica sostanziale l'art. 207, par. 4, TFUE[64].

Dai preamboli degli ACD in esame emergono alcune suggestioni di contesto e di carattere interpretativo. I nuovi accordi sono legati intrinsecamente agli ALS in essere, assieme ai quali dovrebbero dare ulteriore linfa alle aree di libero scambio, in una prospettiva di rinnovata collaborazione a fronte del rapido sviluppo dell'economia e del commercio digitale. L'obiettivo non è unicamente modernizzare e rendere più dinamico il sistema di cooperazione, ma anche «complementing the Parties' international and regional leadership roles in the pursuit of ambitious benchmarks, rules and standards for the digital economy and digital trade»[65]. Guardando alla questione dal piano del diritto e della prassi dell'Unione nel campo della PCC, sembra che sia in atto non tanto una ricerca di *partners* diversi, quanto piuttosto la riorganizzazione dell'assetto multilaterale con *partners* già esistenti.

Posto che i testi dei due ACD sono piuttosto simili, appare subito chiaro che i rispettivi primi Titoli, contenenti disposizioni generali, ricalcano in larga parte, ancorché con qualche ampliamento, lo schema dei capitoli sul commercio digitale di cui agli ALS visti negli ultimi passaggi del paragrafo precedente. Di fatto, si è inteso riproporre il modello più avanzato di regole per ovviare alle carenze delle deboli e scarne disposizioni degli ALS con Corea del Sud e Singapore in materia di commercio elettronico. Insomma, la prima parte di questi ACD altro non è che un allineamento dei rapporti tra parti all'evoluzione dello stato dell'arte[66].

Discorso a tratti diverso per il secondo Titolo (art. 5 ss.) dei due ACD,

---

con Singapore, COM(2023) 230 final, del 14 aprile 2023. Nel documento, la Commissione chiarisce che l'iniziativa è coerente con il riesame della politica commerciale della Commissione del febbraio 2021. Inoltre, nel punto relativo al rispetto del principio di sussidiarietà, viene A norma dell'art. 5, par. 3, TUE, il principio di sussidiarietà si osserva che nella fattispecie non si pongono problemi di sorta, giacché «[l]a politica commerciale comune è un settore di competenza esclusiva dell'Unione ai sensi dell'articolo 3 TFUE».

[64] Council Decision authorising the opening of negotiations for agreements on digital trade disciplines with the Republic of Korea and with Singapore, 8886/23, del 6 giugno 2023. L'atto indica come ulteriore base giuridica (procedurale) l'art. 218, parr. 3 e 4, TFUE. Permangono, semmai, dubbi sull'opportunità di non prevedere ulteriori basi giuridiche sostanziali accanto all'art. 207, par. 4, TFUE: V. REMONDINO, *op. cit*., p. 208 ss.

[65] V., in specie, Preambolo dell'ACD UE-Singapore.

[66] Si vedano anche gli artt. 37 dell'ACD UE-Corea del Sud e 41 dell'ACD UE-Singapore, che specificano le principali modifiche ai corrispondenti ALS.

rinominato "*Digital Trade Disciplines*": a mano a mano che si procede con la lettura (specie dall'art. 16) affiorano disposizioni più strutturate o addirittura del tutto nuove rispetto ai capitoli sul commercio digitale degli ALS conclusi dall'UE. Tra i principali settori sui quali si estende la copertura di ciascun ACD vi sono la fatturazione elettronica, il processo elettronico di trasmissione dei documenti doganali, specifiche dettagliate su pagamenti elettronici. Degna di nota è l'inclusione di disposizioni in materia di cybersicurezza, nonché il riconoscimento dell'importanza di un approccio basato sul rischio e costruito in funzione di buone pratiche comuni, per affrontare minacce *cyber* sempre più sofisticate, incidendo nella minor misura possibile sugli scambi commerciali. Vengono poi poggiate le fondamenta per una collaborazione alla definizione di *standards*, norme tecniche e procedure di valutazione di conformità, tenendo presente l'enfasi riposta dall'Unione su questa priorità[67]. Si assiste anche a un tentativo di rafforzamento della dimensione sociale del commercio digitale, come dimostrano gli articoli che si occupano di inclusione digitale e coinvolgimento dei portatori di interesse.

Tutti questi riscontri vanno però "decodificati" attraverso varie puntualizzazioni risultanti da osservazioni d'insieme e più approfondite.

A ben vedere, permane uno scarto evidente tra lo spettro applicativo dei partenariati digitali e lo spazio d'azione degli accordi in parola, invero molto più ristretto. Sebbene i primi abbiano influenzato la genesi dei secondi, vi è solo una limitata corrispondenza tra i propositi degli strumenti di *soft law* e gli obblighi convenuti in quelli di *hard law*.

Inoltre, l'aumento in senso orizzontale, cioè in termini di estensione del campo di applicazione, degli ACD rispetto alla portata dei capitoli sul commercio digitale degli ALS più significativi nell'economia di questo lavoro, non è controbilanciato da una riduzione del novero di eccezioni ed esenzioni di cui si è detto in precedenza (*supra*, par. 2). Anzi, alcune disposizioni particolarmente significative, come quelle dedicate ai flussi transfrontalieri e alla protezione dei dati, sono ora più lunghe anche perché le parti hanno inteso sottolineare in maniera più decisa alcune prerogative

[67] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Una strategia dell'UE in materia di normazione. Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM(2022) 31 final, 2.2.2022. V. anche A. HARCOURT, *The Global Internet Standard-Setting and Legitimacy Mechanisms in the EU*, in M. ELIANTONIO , A. VOLPATO, S. RÖTTGER-WIRTZ (a cura di), *Global Standards and EU Law. Challenges for the EU Principles of Good Governance*, Cheltenham-Northampton, 2025, p. 68 ss.

a loro favorevoli e potenzialmente restrittive per l'oggetto dell'apposito regime giuridico.

Tale estensione non corrisponde neppure a un'analoga accentuazione del grado di profondità delle regole che si stanno considerando. Detto altrimenti, la vincolatività delle stesse è oltremodo tenue, forse pressoché nulla: lo dimostrano le partizioni degli articoli più pertinenti, che in genere contengono una primo inciso nel quale le parti dichiarano di riconoscere l'importanza di questo o quel settore e un secondo blocco rivolto all'enunciazione di impegni di massima (le espressioni più utilizzate sono «the Parties shall endeavour to» o «shall encourage their respective bodies to»)[68].

Al tempo stesso, e al netto di richiami introduttivi, le disposizioni degli ACD con Corea del Sud e Singapore sono state costruite in chiave squisitamente mercantilistica e appaiono difficilmente sussumibili alla dimensione di tutela dei diritti fondamentali che permea il MUD[69]. È appena il caso di riportare che i principali riferimenti a meccanismi di difesa dei diritti degli individui sono quelli che, nel Preambolo di entrambi gli ACD, conducono alla Dichiarazione Universale dei Diritti Umani del 1948[70], vale a dire uno strumento bel lungi dall'essere in grado di governare efficacemente le istanze e i corrispettivi rischi nell'ecosistema digitale del terzo millennio. Per altro verso, è significativo che gli artt. 38 dell'ACD UE-Corea del Sud e 42 dell'ACD UE-Singapore, precisino che nessuna disposizione «shall be construed as conferring rights or imposing obligations on any persons, other than those rights and obligations created between the Parties under public international law». Siffatti obblighi certamente non possono giustapporsi a quelli che, in ambito UE, derivano dalla (o si rafforzano attraverso la) Carta dei diritti fondamentali.

[68] Tra l'altro, l'art. 38, par. 2, dell'ACL UE-Corea del Sud proibisce a ciascuna parte di ammettere che un singolo possa far valere di fronte a un giudice interno eventuali misure della controparte che non siano in linea con l'accordo.

[69] Come argomentato in dottrina, ciò è pur sempre una conseguenza del c.d. «*soft register*» degli ACD, ritenuto sorprendente perché finisce per riflettere «the Union's decision to pursue a promotional, rather than assertive, strategy in advancing its non-trade values in this regulatory domain»: S. VILLANI, *The EU Digital Trade Instruments and the WTO System*, in E. BARONCINI (a cura di), *The WTO as a Major Driver for Sustainable Development and Its Reform*, Bologna, 2025, p. 131.

[70] UN Resolution A/RES/217(III), 10 dicembre 1948.

4. Accordi di altra natura: tra commercio, associazione e cooperazione allo sviluppo

L'analisi si sposta ora su un altro fronte dell'azione esterna dell'Unione, più indecifrabile rispetto alla PCC. Ci si addentra in una categoria composita, nella quale alcuni autori ricomprendono aree rinominate "Cooperation Policies beyond Trade"[71].

A tale proposito, gli accordi di partenariato economico divengono nuovi elementi di indagine, principalmente per via di alcuni evidenti dati quantitativi. Poiché lo scopo degli APE è sostenere lo sviluppo dei *partners* commerciali dell'area Africa, Caraibi e Pacifico (ACP), l'Unione ha concluso molti accordi di questo tipo nell'ultimo ventennio, complessivamente più di 70[72], divenendo una delle controparti privilegiate di tali paesi[73].

Più precisamente, gli APE sono le principali cornici giuridiche facenti capo all'accordo di Cotonou del 2000[74], che dal suo canto costituiva il quadro generale d'azione dell'UE nell'area interessata. Ai sensi dell'accordo di Cotonou (artt. 36 e seguenti), le parti hanno convenuto di concludere nuovi accordi commerciali compatibili con le regole OMC, eliminando progressivamente gli ostacoli al commercio e rafforzando la cooperazione in tutti i settori rilevanti per il commercio[75].

Ciononostante, occorre precisare che il "sistema Cotonou" tende ad allontanarsi progressivamente dalla sfera della PCC, per installarsi anche – e, forse, soprattutto – altrove nell'ampia superficie dell'azione esterna dell'Unione. L'accordo di Cotonou è di fatto basato sull'art. 310 TCE,

[71] J. WOUTERS, F. HOFFMEISTER, G. DE BAERE, T. RAMOPOULOS (a cura di), *op. cit*., p. 289 ss.

[72] Anche per questo motivo tale modello di accordi è stato definito unico nel suo genere: E. PICHON, *After Cotonou: Towards a New Agreement with the African, Caribbean and Pacific States* (EPRS - European Parliamentary Research Service, 2021), p. 2.

[73] M. FERRARI, *L'azione dell'Unione europea sul palco internazionale: le clausole di tutela dei diritti umani negli accordi con gli Stati dell'Africa, dei Caraibi e del Pacifico (ACP),* in *I Post di AISDUE*, 3 luglio 2022, p. 513.

[74] Accordo di partenariato tra i membri del gruppo degli stati dell'Africa, dei Caraibi e del Pacifico, da un lato, e la Comunità europea e i suoi Stati membri, dall'altro, firmato a Cotonu il 23 giugno 2000, in GUUE del 15 dicembre 2000, L 317/3.

[75] Per quanto riguarda il contenuto degli APE, l'art. 37, par. 7, dell'accordo di Cotonou prevedeva che la liberalizzazione degli scambi, da parte dell'UE, si basasse sull'*acquis* e fosse intesa a migliorare quelle che all'epoca erano le attuali condizioni di accesso dei paesi ACP al mercato. L'art. 37, par. 5, precisava comunque che i negoziati per gli APE avrebbero dovuto essere avviati con i paesi ACP che si consideravano «pronti a compiere tale passo», al livello che essi ritenevano adeguato e conformemente alle procedure concordate dal gruppo di Stati ACP, «tenendo conto del processo d'integrazione regionale in atto tra gli Stati ACP».

l'equivalente dell'attuale art. 217 TFUE[76], ma è sempre stato considerato come tangibile espressione della politica UE di cooperazione allo sviluppo *ex* artt. 208 e ss. TFUE[77]; una politica, questa, da tempo multidimensionale e a vocazione globale, che spicca per la differenziazione degli strumenti giuridici e finanziari e per il ricorso a basi giuridiche diverse da quelle specificamente previste dal titolo del TFUE denominato "Cooperazione con i paesi terzi e aiuto umanitario"[78]. Il collegamento di cui si sta discutendo è invero acclarato non solo nella prassi UE[79], ma anche in dottrina[80]. Inoltre, basta leggere l'art. 19 dell'accordo per constatare che uno degli obiettivi primari era la riduzione e la definitiva eliminazione della povertà, il che corrisponde esattamente alla missione della politica UE di cooperazione allo sviluppo[81].

Queste constatazioni non sono meramente cosmetiche, perché mentre

---

[76] Secondo tale articolo «[l]'Unione può concludere con uno o più paesi terzi o organizzazioni internazionali accordi che istituiscono un'associazione caratterizzata da diritti ed obblighi reciproci, da azioni in comune e da procedure particolari».

[77] Sul rapporto tra PCC e politica UE di cooperazione allo sviluppo si veda, segnatamente, S. GSTÖHL, *Tightening the EU's Trade- Development Nexus. A Strategic Turn in Search for Enhanced Effectiveness*, in M. HAHN, G. VAN DER LOO (a cura di), *op. cit*., p. 383 ss.

[78] P. IANNUCCELLI, *Artt. 208-213 TFUE*, in A. TIZZANO (a cura di), *op. cit*., p. 1718.

[79] Documento *Partnership Agreement. ACP-EC. Signed in Cotonou on 23 June 2000. Revised in Luxembourg on 25 June 2005* (2007), pubblicato dalla Commissione europea, Direzione Generale per lo sviluppo e le relazioni con gli Stati ACP (disponibile al seguente indirizzo *Internet:*https://eur-lex.europa.eu/resource.html?uri=cellar:b856d1b1-d939-4c4a-8ff2-64a7fd482fb5.0002.02/DOC_1&format=PDF). Si veda anche https://eur-lex.europa.eu/EN/legal-content/summary/eu-development-policy.html.

[80] B. MARTENCZUK, *From Lomé to Cotonou: The ACP–EC Partnership Agreement in a Legal Pespective,* in *European Foreign Affairs Review*, 2000, p. 461 ss.; P. HIPOLD, *EU Development Cooperation at a Crossroads: The Cotonou Agreement of 23 June 2000 and the Principle of Good Governance*, in *European Foreign Affairs Review*, 2002, p. 53 ss.; S. BARTLET, *ACP-EU Development Cooperation at a Crossroads? One Year after the Second Revision of the Cotonou Agreement,* in *European Foreign Affairs Review*, 2012, p. 1 ss.; M. P. BROBERG, *Don't Mess with the Missionary Man! On the Principle of Coherence, the Missionary Principle and the European Union's Development Policy*, in P. J. CARDWELL (a cura di), *EU External Relations Law and Policy in the Post-Lisbon Era*, The Hague, 2012, p. 192 ss.; M. CARBONE, *Rethinking ACP-EU Relations After Cotonou: Tensions, Contradictions, Prospects,* in *Journal of International Development*, 2013, p. 742 ss.; P. LEINO, *Administering EU Development Policy: Between Global Commitments and Vague Accountability Structures,* in *European Papers*, 2017, p. 617 ss.; M. FURNESS, L. A. GHICA, S. LIGHTFOOT, B. SZENT-IVÁNYI, *EU Development Policy: Evolving as an Instrument of Foreign Policy and as an Expression of Solidarity,* in *Journal of Contemporary European Research*, 2020, p. 89 ss.

[81] In aggiunta, nel Preambolo le parti esprimono la volontà di rivitalizzare la loro «relazione particolare, dandole un carattere globale e integrato per costruire un partenariato forte, basato sul dialogo politico, sulla cooperazione allo sviluppo e sulle relazioni economiche e commerciali». L'art. 20, inerente alla metodologia, enuncia le strategie integrate volte a perseguire obiettivi di cooperazione allo sviluppo.

nel settore della PCC l'Unione ha una competenza esclusiva (art. 3 TFUE), la cooperazione allo sviluppo, che comunque sembra possedere un ambito applicativo alquanto vasto[82], dipende da un regime di competenze peculiare (art. 4, par. 4, TFUE), contraddistinto da un margine di intervento residuale dell'Unione rispetto ai poteri di gestione degli Stati membri[83]. In via ulteriore, l'essenza della politica di cooperazione allo sviluppo si rispecchia (o almeno dovrebbe) nelle esigenze di rispetto dei diritti fondamentali, in parte anche a causa dell'influenza di varie regole di derivazione internazionale relative al diritto allo sviluppo[84].

Esaminando i testi di molti APE attualmente in vigore, si nota però l'assenza di capitoli o anche solo disposizioni riferibili al commercio digitale[85]. Da un lato, ciò non sorprende più di tanto, poiché la matrice di riferimento – l'accordo di Cotonou, appunto – era stata definita in un momento in cui la transizione dall'analogico al digitale era ancora lontana dall'essere completata. D'altro canto, non si può sottovalutare il fatto che le stesse carenze persistano grossomodo in tutti gli APE che l'Unione ha concluso con Stati ACP dopo il lancio della prima strategia sul MUD[86]. Al massimo, pare che regole più specifiche, anche sotto forma di impegni, saranno discusse nel corso di cosiddetti "negoziati di modernizzazione"

---

[82] V. in particolare Corte giust., 11 giugno 2014, causa C-377/12, *Commissione c. Consiglio*, ECLI:EU:C:2014:1903. Cfr. anche M. BROBERG, R. HOLDGAARD, *Demarcating the Union's Development Cooperation Policy after Lisbon: Commission V. Council (Philippines PCFA),* in *Common Market Law Review*, 2015, p. 547 ss.

[83] P. DE PASQUALE, F. FERRARO, *Manuale di diritto dell'Unione europea / Giuseppe Tesauro*, Editoriale Scientifica 2023, p. 75. Si è poi affermato che «development cooperation is carved out as what could be called a 'non-principal' area of shared competence. This apparent lower ranking of development cooperation contributes to its 'low politics' status among the other policy areas of EU external relations» (P. J. CARDWELL, D. JANČIĆ, *The European Parliament and Development Cooperation: Democratic Participation in the 'Low Politics' of EU External Relations*, in *Journal of European Integration*, 2019, p. 369).

[84] F. CHERUBINI, *I valori dell'Unione europea nella politica di cooperazione allo sviluppo,* in E. SCISO, R. BARATTA, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2016, p. 120 ss.

[85] L'eccezione più significativa è costituita dall'Accordo di partenariato economico tra gli Stati del CARIFORUM, da una parte, e la Comunità europea e i suoi Stati membri, dall'altra, in GUUE del 30 ottobre 2008, L 289/3 (Artt. 119 e 129, che però sono da considerarsi come precursori rispetto ai corrispettivi degli ALS con Corea del Sud e Canada).

[86] Ad esempio: Accordo di partenariato economico tra l'Unione europea e i suoi Stati membri, da una parte, e gli Stati della SADC aderenti all'APE, dall'altra, in GUUE del 19 giugno 2016, L 250/3; Accordo di partenariato economico tra l'Unione europea, da una parte, e la repubblica del Kenya, membro della comunità dell'Africa orientale, dall'altra, in GUUE dell'1 luglio 2024, L, 2024/1648.

avviati dall'UE in relazione ad alcuni accordi esistenti con paesi terzi[87].

Vi sono tuttavia aggiornamenti abbastanza significativi, riguardanti l'approccio dell'UE alla cooperazione allo sviluppo, che potrebbero indurre a intravedere spiragli di cambiamento.

Il 15 novembre 2023, a Samoa, l'Unione e gli Stati membri hanno concluso un nuovo accordo di partenariato con i membri dell'Organizzazione degli Stati ACP[88]. L'accordo di Samoa è stato applicato in via provvisoria dal gennaio 2024 e dovrebbe costituire il regime *post*-Cotonou per due decenni, sostituendo così il precedente quadro generale per le relazioni dell'UE con i paesi ACP.

Il baricentro dell'accordo di Samoa rimane la cooperazione allo sviluppo, analogamente a quanto visto per l'accordo di Cotonou, e sempre per i motivi anzidetti. In linea con quest'ultimo, il nuovo quadro UE-ACP richiede alle parti di basarsi sui regimi commerciali preferenziali esistenti e sugli APE come strumenti fondamentali della loro cooperazione commerciale[89].

Una delle innovazioni più nitide dell'accordo di Samoa è che con esso viene aperta la strada a un nuovo approccio dell'UE nei confronti delle questioni relative al digitale, presentate come pietre miliari dello sviluppo dei paesi ACP, con particolare attenzione agli Stati africani. Già nel preambolo, ad esempio, si sottolinea l'importante ruolo della scienza, della tecnologia, della ricerca e dell'innovazione «nell'accelerare la transizione verso società basate sulla conoscenza, facilitata dall'uso di strumenti digitali ai fini dello sviluppo sostenibile». Alcune disposizioni dell'accordo, poi, consentono di comprendere meglio questa tendenza.

La digitalizzazione è inizialmente presentata come uno strumento per lo sviluppo di società inclusive e pluralistiche; le parti (art. 11) hanno

[87] È il caso, ad esempio, dell'APE UE-Africa orientale e meridionale.

[88] Accordo di partenariato tra l'Unione europea e i suoi Stati membri, da una parte, e i membri dell'Organizzazione degli Stati dell'Africa dei Caraibi e del Pacifico, dall'altra, in GUUE del 28 dicembre 2023, L 2023/2862. Sull'Accordo di Samoa si veda M. LANGAN, S. PRICE, *The Frustrations of Free Trade and the Africa–European Union Samoa Agreement*, in *Journal of Developing Societies*, 2025, p 7 ss.

[89] Art. 50 dell'Accordo di Samoa, ove si legge altresì che le parti «sottolineano l'importanza degli scambi commerciali nelle loro relazioni generali e si impegnano a promuovere l'intensificazione e la diversificazione dei flussi commerciali a vantaggio di entrambe», in particolare in vista dell'integrazione delle economie dei membri dell'organizzazione degli Stati ACP nelle catene del valore regionali e mondiali; si aggiunge che «la cooperazione commerciale sia condotta conformemente al sistema commerciale multilaterale basato su regole al fine di promuovere scambi liberi, equi e aperti per conseguire una crescita e uno sviluppo sostenibili».

convenuto di adoperarsi per sfruttare appieno il potenziale delle soluzioni digitali al fine di promuovere obiettivi democratici quali la parità di accesso del pubblico alle informazioni a tutti i livelli e il processo decisionale partecipativo. Successivamente, la digitalizzazione viene definita come un motore per promuovere la trasformazione economica, lo sviluppo del settore privato e il progresso industriale per una crescita inclusiva e sostenibile (artt. 43 e 44), poiché le parti hanno riconosciuto «il ruolo centrale dell'economia digitale quale amplificatore e acceleratore del cambiamento, in grado di stimolare una diversificazione economica significativa, creare posti di lavoro e consentire alla crescita di compiere un netto balzo in avanti» (art. 48). L'accordo propone anche una serie di collegamenti tra la digitalizzazione e i pilastri dello sviluppo sostenibile: tra i settori di riferimento figurano la pubblica amministrazione (art. 13), l'istruzione (art. 28), la sanità (art. 29) e la partecipazione dei giovani alla società (art. 35).

Esiste anche una disposizione specifica sulle tecnologie dell'informazione e della comunicazione (TIC) e sull'economia digitale: è l'art. 48, contenuto nel capitolo 3 dell'accordo, che a sua volta riguarda la scienza, la tecnologia, l'innovazione e la ricerca. Gli obiettivi individuati nell'art. 48 sono, in particolare, ridurre il divario digitale, consentire un facile accesso alle TIC, garantire una maggiore complementarità e armonizzazione dei sistemi di comunicazione e il loro adeguamento alle nuove tecnologie, promuovere e sostenere l'imprenditoria digitale, sviluppare e gestire politiche di tutela della *privacy* e dei dati, promuovere misure volte a facilitare i flussi di dati e sostenere il quadro normativo per promuovere la produzione, la vendita e la fornitura di prodotti e servizi digitali. Disposizioni addizionali sono previste anche nei tre protocolli regionali aventi rispettivamente ad oggetto ciascuna delle tre macroaree geografiche interessate.

Tanto detto, è pur sempre il caso di rappresentare che molte delle disposizioni richiamate non introducono obblighi realmente prescrittivi, men che meno giustiziabili, atteso che l'accordo di Samoa definisce un quadro di riferimento generale: è sufficiente leggere alcuni riferimenti testuali (le parti, «riconoscono», «affermano», «si impegnano», «cooperano») per realizzare che questo strumento non potrà essere determinante in via esclusivamente autonoma per un significativo cambiamento di passo nelle relazioni giuridiche tra l'UE e gli Stati ACP nel campo del digitale. Tuttavia, si ritiene che in quest'ambito l'accordo di

Samoa possa comunque divenire il presupposto per eventuali sviluppi materiali di un certo rilievo nel processo di costruzione e messa a sistema dei rapporti instaurati dall'Unione al di fuori del *noyau dur* della PCC: occorrerà dunque monitorarne l'attuazione, in particolare attraverso la reinterpretazione e l'eventuale aggiornamento degli attuali APE o la conclusione di APE più moderni.

5. Strumenti diversi dagli accordi: tra intese informali e leve finanziarie

Stanti gli evidenti limiti degli accordi sui quali ci si è concentrati nei paragrafi precedenti, almeno per quanto riguarda le reali prospettive di proiezione della normativa digitale dell'Unione all'esterno, si considera opportuno spostare il piano di analisi verso elementi di prassi di altra natura, allo scopo di verificare se la dimensione esterna del MUD possa essere plasmata, anche solo in parte, ricorrendo a strumenti *sui generis*.

Per elaborare questo passaggio, si ritiene particolarmente indicativo focalizzare l'attenzione sul continente africano. L'Africa da qualche tempo è al centro di un apposito e ambizioso programma UE di cooperazione[90]. Parallelamente, la già citata Strategia sull'affermazione di una politica commerciale aperta, sostenibile e assertiva sottolinea l'esigenza di rafforzare i partenariati dell'UE con Stati terzi; sennonché, fatta eccezione per quelli che ricadono nell'area del vicinato o nel gruppo dei candidati all'adesione, l'attenzione è diretta in via assolutamente prioritaria ai paesi africani[91].

A ben vedere, la centralità dell'Africa in quest'ottica ha una sua ragion d'essere. Oltre agli storici legami che collegano tale continente al processo di integrazione europea[92], l'Africa è per l'Unione europea un soggetto di spiccato rilievo commerciale. È infatti risaputo che all'interno dell'Unione Africana (UA) è stata istituita l'Area continentale di libero scambio per l'Africa (AfCFTA), che ad oggi è la più grande zona di libero scambio del mondo. Inutile dire che le relazioni commerciali tra UE e Africa dipendono

[90] Comunicazione congiunta della Commissione e dell'Alto Rappresentante al Parlamento europeo e al Consiglio, *Verso una strategia globale per l'Africa*, JOIN(2020) 4 final, 9.3.2020.

[91] COM(2021) 66 final, cit., p. 18 ss.

[92] A tale proposito, si ricorda che un passaggio della Dichiarazione *Schuman* del 1950 include tra i compiti essenziali dell'Europa lo sviluppo del continente africano. Di conseguenza, il Trattato di Roma del 1957 che istituiva la Comunità economica europea disponeva un'associazione con i territori d'oltremare (Parte IV), molti dei quali erano paesi africani (Allegato IV).

largamente dalle interconnessioni tra il mercato interno dell'Unione e l'AfCFTA. Va da sé che l'evoluzione dei settori digitali è fondamentale per lo sviluppo di un mercato ricompreso in un continente contrassegnato dall'elevatissimo numero di abitanti e dalla popolazione più giovane del pianeta. La prassi sta mostrando segnali interessanti a questo proposito[93].

Eppure, si è visto poc'anzi che le relazioni UE-Africa in materia di digitale non vengono sviluppate tramite gli strumenti giuridici tipicamente utilizzati per regolamentare in via pattizia le relazioni commerciali. Diversamente, rilevano soprattutto iniziative di natura strategica e finanziaria.

L'Unione ha intensificato la promozione di modelli di cooperazione *soft*, in linea con il programma proposto da Ursula von der Leyen nel 2019, in cui l'Africa è descritta come un obiettivo fondamentale per le opportunità politiche, economiche e di investimento[94]. In particolare, con la Strategia globale per l'Africa del 2020, la Commissione ha annunciato l'intenzione di costruire un partenariato per la trasformazione digitale al fine di stimolare riforme e investimenti adeguati a sostegno della creazione di un Mercato Unico Digitale africano[95]. Poco dopo, altre istituzioni politiche dell'UE hanno agito per ribadire questo intento. Il Consiglio ha pubblicato conclusioni su un partenariato più forte per l'Africa, in cui ha proposto la sua concezione di un'economia digitale inclusiva derivante (tra l'altro) dal sostegno europeo all'ambizione digitale dell'Africa: le conclusioni sottolineano la centralità della cooperazione su sicurezza informatica e integrità democratica, nonché l'importanza di partecipare al commercio digitale[96]. Il Parlamento europeo ha invece enfatizzato il legame tra digitalizzazione, inclusione e sviluppo: in una risoluzione adottata nel 2021, l'argomento in questione è stato inserito in un contesto più ampio, che riflette sostanzialmente i pilastri principali dello sviluppo

[93] Ad esempio, l'Africa è *leader* mondiale nei pagamenti mobili, e lo sviluppo dei servizi bancari mobili e digitali ha permesso a milioni di africani di accedere a finanziamenti Si vedano anche i dati riportati qui https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa.

[94] Documento "*A Union that strives for more. My agenda for Europe*", 2019, disponibile al seguente indirizzo *Internet*: https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf (spec. p. 18).

[95] JOIN(2020) 4 final, *cit*. In particolare, la strategia indica la necessità di elaborare un solido quadro normativo in settori quali la protezione dei dati e dei consumatori, i servizi finanziari digitali, la criminalità informatica e l'*e-governance*.

[96] Conclusioni del Consiglio del 30 giugno 2020, doc. 9265/20.

sostenibile[97].

Concretamente, alla fine del 2018 è stata istituita una *task force* UE-UA sull'economia digitale con l'obiettivo di creare una piattaforma di partenariato per il settore privato, i donatori, le organizzazioni internazionali, le istituzioni finanziarie e la società civile[98]. L'idea era quella di promuovere una visione condivisa, una serie di principi comuni concordati e un elenco di azioni incentrate sugli obiettivi fondamentali legati al digitale. Tra i principali risultati del lavoro della *task force* vi è una serie di raccomandazioni politiche[99]. È stata poi avviata una *partnership* tra UE e Africa sull'economia digitale, che accenna in linea teorica all'obiettivo di to creare un ALS «*continent-to-continent*» muovendo dallo stato dell'arte dell'AfCFTA. Ciononostante, questo proposito sembra rimanere sullo sfondo rispetto ad altre iniziative, dal momento che la *partnership* allude anche ad accordi intergovernativi e punta con decisione alla definizione di generici partenariati, alla realizzazione di cospicui investimenti e alla finalizzazione riforme interne nel continente africano[100].

Di particolare impatto è stato il lancio della strategia *Global Gateway* alla fine del 2021[101]. La *Global Gateway* ha aperto la strada alla mobilitazione di 300 miliardi di euro di investimenti in tutto il mondo attraverso l'Unione europea, i suoi Stati membri – comprese le loro

---

[97] Risoluzione del Parlamento europeo del 25 marzo 2021 su una nuova strategia UE-Africa — un partenariato per lo sviluppo sostenibile e inclusivo (2020/2041(INI)). Anche se il nesso con il commercio non è esplicitamente indicato nella sezione della relazione dedicata alla digitalizzazione dell'Africa, resta il fatto che il Parlamento europeo ha esortato l'UE a contribuire a questa transizione nel tentativo di apportare un valore aggiunto ai paesi africani (e alle loro popolazioni).

[98] Per maggiori informazioni si veda anche https://digital-strategy.ec.europa.eu/it/node/1744.

[99] Le raccomandazioni si innestano sui seguenti assi: accelerare il raggiungimento dell'accesso universale alla banda larga a prezzi accessibili, garantire competenze essenziali per tutti (nell'istruzione e nella formazione professionale) per consentire ai cittadini di prosperare nell'era digitale, migliorare il contesto imprenditoriale e facilitare l'accesso ai finanziamenti e ai servizi di sostegno alle imprese per promuovere l'imprenditorialità digitale, accelerare l'adozione dei servizi elettronici e l'ulteriore sviluppo dell'economia digitale per il raggiungimento degli obiettivi di sviluppo sostenibile.

[100] V. più nel dettaglio il documento "*New Africa-Europe Digital Economy Partnership*", disponibile al seguente indirizzo *Internet*: https://international-partnerships.ec.europa.eu/system/files/2021-01/new-africa-eu-digital-economy_en_0.pdf.

[101] Comunicazione congiunta della Commissione e dell'Alto Rappresentante al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Il Global Gateway*, JOIN(2021) 30 final, 1.12.2021.

agenzie di attuazione e le banche pubbliche di sviluppo –, la Banca europea per gli investimenti (BEI) e la Banca europea per la ricostruzione e lo sviluppo (BERS). Di conseguenza, la *Global Getaway* potrebbe essere vista come una "cinghia di trasmissione" tra la strategia globale per l'Africa e la sua dimensione operativa, caratterizzata dalla fornitura di risorse economiche guidate dall'UE per sostenere progetti rilevanti (circa 150 miliardi di euro per investimenti nei paesi africani)[102]. Il digitale è una priorità assoluta della *Global Gateway*[103]: in particolare, la strategia annuncia che «l'UE offrirà pacchetti per l'economia digitale che associeranno gli investimenti infrastrutturali all'assistenza a livello di paese per garantire la protezione dei dati personali, la cibersicurezza e il diritto alla tutela della vita privata, un'intelligenza artificiale affidabile e mercati digitali equi e aperti»[104]. Ciò detto, sono diverse le iniziative attuate sotto l'egida della *Global Gateway*[105].

Dai rilievi appena effettuati è possibile formulare talune riflessioni, collocando il *modus operandi* dell'Unione in un panorama più ampio, financo di sistema.

La prima impressione è che il perseguimento in ambito esterno di obiettivi associati al MUD dipenderà in misura crescente da strumenti

---

[102] Si veda più nel dettaglio G. CASANO, E. PANIZZA, *The Global Gateway Africa-Europe Investment Package and the Future of EU-AU Relations*, in A. O. AKINOLA, E. ASIGE LIAGA (a cura di), *Development and Regional Stability in Africa: Unlocking Potential*, Cham, 2024, p. 215 ss.

[103] V. anche C. TEEVAN, E. DOMINGO, *The Global Gateway and the EU as a Digital Actor in Africa* (ECDPM, Discussion Paper n. 332, 2022 disponibile al seguente indirizzo *Internet*: https://ecdpm.org/application/files/9316/6962/8500/Global-Gateway-EU-digital-actor-Africa-ECDPM-Discussion-Paper-332-2022.pdf).

[104] JOIN(2021) 30 final, cit., p. 4

[105] Ad esempio, il *Digital for Development (D4D) Hub*, una piattaforma strategica creata per promuovere la cooperazione digitale tra l'UE (e i suoi Stati membri) e i *partner* ACP, con la missione di promuovere un approccio alla trasformazione digitale incentrato sull'uomo (https://d4dhub.eu/). Inoltre, l'UE e la *Smart Africa Alliance* (una rete di paesi africani, organizzazioni internazionali e attori del settore privato globale) hanno firmato un accordo amministrativo e un accordo di sovvenzione per progettare e attuare iniziative volte a colmare il divario digitale in Africa: ad esempio, attraverso la diffusione di reti digitali, il potenziamento dei servizi di *e-governance* e lo studio del potenziale dell'intelligenza artificiale (https://smartafrica.org/global-gateway-eu-and-smart-africa-strengthen-partnership-for-africas-digital-transformation/). Per diversi anni l'UE ha pure contribuito alla *Policy and Regulation Initiative for Digital Africa* (PRIDA), un'iniziativa congiunta realizzata con l'UA e l'Unione internazionale delle telecomunicazioni per affrontare priorità chiave come la domanda e l'offerta di banda larga e lo spazio di *governance* di Internet in Africa (https://international-partnerships.ec.europa.eu/policies/programming/programmes/policy-and-regulation-initiative-digital-africa-prida_en).

diversi dagli accordi. Ma se molteplici iniziative UE di un certo rilievo sono ancorate a forme di cooperazione piuttosto indecifrabili e dalla natura ibrida, si apre un campo di gioco che rischia di presentare prevedibili vuoti di controllo o nel quale l'*accountability* dell'Unione si confonderebbe con quella degli Stati membri e di varie possibili controparti, come alcuni Stati terzi, piuttosto che organizzazioni di Stati (ad esempio, l'Unione Africana) o ulteriori entità regionali. Dal punto di vista giuridico, la mancanza di schemi formali come quelli alla base delle categorie di accordi internazionali previste dal TFUE complica inevitabilmente una situazione già di per sé intricata, se non altro perché si opacizzano le coordinate di intervento delle istituzioni dell'Unione: si pensi alla marginalizzazione del Parlamento europeo, o al possibile aumento di interventi degli Stati membri al di fuori del Consiglio, per tacere dell'impossibilità della Corte di giustizia di svolgere qualsivoglia funzione di garanzia del rispetto del diritto UE, ad esempio in forza dell'art. 218, ultimo comma, TFUE.

Per l'effetto, si indeboliscono i presupposti per assicurare che siano trasferiti e promossi efficacemente non solo gli obiettivi connaturati all'evoluzione del MUD, ma anche i principi richiamati dall'art. 21 TUE. Proprio a quest'ultimo riguardo, la sensazione sembra essere più che mai fondata. Un recente studio ha dimostrato che la maggior parte dei progetti della strategia *Global Gateway* vanno ad esclusivo vantaggio di poche imprese europee, mentre i paesi terzi sono spesso esclusi dai processi decisionali e di definizione delle priorità[106]. In presenza di una simile situazione, gli obiettivi (esterni) perseguiti dall'Unione nel campo del digitale – sempre ammesso che possano essere avvicinati – assumerebbero declinazioni che entrerebbero in rotta di collisione con linee rosse particolarmente sensibili dell'ordinamento giuridico UE, in quanto riconducibili all'esercizio e – in una certa misura – all'attribuzione delle competenze.

C'è poi la questione dell'utilizzo delle risorse da investire e della trasparenza in merito. Su questo fronte, le problematiche che possono originarsi sono essenzialmente due.

La prima riguarda l'alimentazione dei canali che fanno scorrere il flusso di finanziamenti verso i beneficiari, in quanto i criteri di fondo sono

---

[106] "*Who profits from the Global Gateway? The EU's New Strategy for Development Cooperation*" (Counter Balance, Eurodad e Oxfam, 2024), disponibile al seguente indirizzo *Internet* https://oi-files-d8-prod.s3.eu-west-2.amazonaws.com/s3fs-public/2024-10/Who%20Profits%20From%20The%20Global%20Gateway%20-%20Report%20Final.pdf.

di difficile lettura. Tale aspetto diventa più marcato in considerazione delle connessioni, più o meno nitide, tra certe iniziative in programma e la politica UE di cooperazione allo sviluppo, che amplifica il margine di manovra degli Stati membri.

La seconda problematica, peraltro correlata alla prima, è rappresentata dai probabili contraccolpi alle esigenze di trasparenza da soddisfare. Vi sono, in realtà, precedenti analoghi che inducono a riflettere e che riguardano iniziative UE nel continente africano, come la gestione del Fondo fiduciario di emergenza per l'Africa quale caposaldo del processo di esternalizzazione delle frontiere dell'Unione. Ebbene, oggi come allora si ripropone il tema dell'origine e delle sorti delle risorse messe a disposizione dall'UE[107], e anche nello specifico divengono indicative le conclusioni tratte dalla Corte dei conti europea[108]. Segnatamente, l'istituzione ha evidenziato criticità circa l'utilizzo Fondo europeo per lo sviluppo sostenibile Plus (EFSD+)[109], che è il principale vettore finanziario della strategia *Global Gateway*, lamentando contrasti con il Regolamento (UE) 2021/947[110], dovuti, in specie, a lacune informative diffuse e scarse garanzie per i reclami delle controparti pertinenti.

6. Ulteriori considerazioni in prospettiva, alla luce della recente Strategia digitale internazionale dell'Unione europea

Gli spunti emersi in trattazione fino a questo momento paiono

---

[107] L. DEN HERTOG, *EU Budgetary Responses to the 'Refugee Crisis': Reconfiguring the Funding Landscape* (CESP Paper in Liberty and Security n, 93/2016, disponibile al seguente indirizzo internet: https://cdn.ceps.eu/wp-content/uploads/2016/05/LSE%20No%2093%20LdH%20on%20EU%20Budgetary%20Responses%20to%20the%20Refugee%20Crisis.pdf).

[108] L'istituzione si era già espressa in termini negativi sulla gestione del Fondo fiduciario per l'Africa: Corte dei conti europea, relazione speciale 32/2018, Il fondo fiduciario di emergenza dell'Unione europea per l'Africa: flessibile, ma non sufficientemente mirato, e relazione speciale 17/2024, Fondo fiduciario dell'UE per l'Africa. Nonostante i nuovi approcci, il sostegno resta non sufficientemente mirato. Anche il Parlamento europeo ha contestato la gestione dello strumento in questione: v. Risoluzione del Parlamento europeo del 13 settembre 2016 sul Fondo fiduciario dell'UE per l'Africa: le implicazioni per lo sviluppo e gli aiuti umanitari (2015/2341(INI)).

[109] Corte dei conti europea, Parere 03/2024 (presentato in virtù dell'art. 287, par. 4, TFUE) che accompagna la valutazione operata dalla Commissione sulla garanzia per le azioni esterne [COM(2024) 208].

[110] Regolamento (UE) 2021/947 del Parlamento europeo e del Consiglio, del 9 giugno 2021, che istituisce lo strumento di vicinato, cooperazione allo sviluppo e cooperazione internazionale – Europa globale, che modifica e abroga la decisione n. 466/2014/UE del Parlamento europeo e del Consiglio e abroga il regolamento (UE) 2017/1601 del Parlamento europeo e del Consiglio e il regolamento (CE, Euratom) n. 480/2009 del Consiglio, in GUUE del 14 giugno 2021, L 209/1.

destinati a trovare declinazioni aggiuntive nel corso dell'evoluzione dell'ultima iniziativa UE di maggior rilievo, vale a dire la Strategia digitale internazionale dell'Unione europea (SDIUE), lanciata nel giugno 2025 da Commissione e Alto Rappresentante[111]. È attraverso il prisma di questa strategia che si possono immaginare avanzamenti delle traiettorie della dimensione esterna del MUD messe in risalto sinora.

La SDIUE parte da un presupposto che permette di apprezzare da subito la rimodulazione tematica delle relazione esterne dell'Unione europea: viene infatti specificato che il digitale rappresenta ora il «fulcro» dell'azione esterna UE[112]. Non si tratta quindi di una strategia di mero aggiornamento, bensì di un vero e proprio snodo, almeno sul piano politico e programmatico, che necessita inevitabilmente di concretizzazione tramite strumenti giuridici idonei. Ciò a maggior ragione se si considera che la SDIUE ripropone il sostegno «irremovibile» dell'UE alla costruzione di «un ordine mondiale basato su regole, in linea con i valori della democrazia, dello Stato di diritto e dei diritti fondamentali»[113], in conformità alle basi fondanti dell'autonomia strategica e della sovranità tecnologica europee. I tre pilastri della SDIUE sono la competitività, la sicurezza economica e la capacità di difesa[114]. Gli ambiti materiali prioritari da affrontare nei rapporti che, secondo la strategia, l'Unione dovrà potenziare o costruire sono sei: infrastrutture digitali sicure e affidabili, tecnologie emergenti, cibersicurezza, manipolazione delle informazioni e ingerenze da parte di attori stranieri, identità digitali e infrastrutture pubbliche digitali, piattaforme *online*.

Da una più attenta lettura della SDIUE, nondimeno, vengono suscitati interrogativi sulla visione sovranazionale che si sta sviluppando in ordine alle relazioni giuridiche che dovrebbero governare il multilateralismo.

Si vuole in prima battuta rimarcare la funzione quasi assistenziale che l'Unione dovrebbe assicurare ai *partners*, in ragione della propria (autoattribuita) *leadership* nei settori chiave di intervento e della sua (autoattribuita) affidabilità come controparte. Queste asserzioni stupiscono

---

[111] Comunicazione congiunta della Commissione e dell'Alto Rappresentante al Parlamento europeo e al Consiglio, *Una strategia digitale internazionale per l'Unione europea*" JOIN(2025) 140 final, 5.6.2025.

[112] *Ibid*., p. 1.

[113] *Ibid*.

[114] In questo senso, la SDIUE in parte attinge dalla Strategia UE sulla sicurezza economica: Comunicazione congiunta della Commissione e dell'Alto Rappresentante al Parlamento europeo e al Consiglio, *sulla Strategia europea sulla sicurezza economica,* JOIN(2023) 20 final, 20.6.2023.

se non altro per via dei conclamati ritardi nella produzione e nell'applicazione di tecnologia da parte dell'Unione e degli Stati membri. Si tratta di divari che anche nel testo della SDIUE vengono presentati come manifesti, coincidendo con lacune che stentano ad essere colmate attraverso le leve del mercato, della politica industriale, della ricerca e dello sviluppo. Per giunta, almeno laddove in gioco vi siano accordi internazionali, affiorano questioni che si rivelano spesso problematiche agli occhi dei *partners*. Basti pensare alla diffidenza nei confronti del *treaty-making process* previsto dal diritto e dalla prassi dell'Unione[115] e agli effetti potenzialmente paralizzanti che potrebbero discendere dall'esercizio delle proprie funzioni di controllo da parte della Corte di giustizia[116].

Rimane il fatto che se con la SIDUE sarà ulteriormente alimentata l'attitudine dell'Unione a ergersi a sostenitore (anche) della transizione digitale a favore di chi sia disposto a seguire il proprio disegno si consoliderà un approccio prevalentemente unidirezionale che probabilmente finirà per restringere il campo di selezione a potenziali *partners* diversi da quelli che hanno raggiunto una reale posizione di vertice nello sviluppo e nell'utilizzo delle tecnologie emergenti. Per quanto concerne la dimensione esterna del MUD, questa rimodulazione potrebbe segnare un'accelerazione dello spostamento del baricentro dalla PCC ad altri settori dell'azione esterna. Tale sentore sembra trovare conferme proprio in alcuni passaggi della SDIUE. Tenendo a mente che la

---

[115] Per spunti di riflessione sull'argomento si rinvia a I. BOSSE-PLATIÈRE, C. RAPOPORT (a cura di), *The Conclusion and Implementation of EU Free Trade Agreements: Constitutional Challenges*, Cheltenham-Northampton, 2019; M. CHAMON, I. GOVAERE (a cura di), *EU External Relations Post-Lisbon The Law and Practice of Facultative Mixity*, Leiden-Boston, 2020.

[116] Ciò anche al netto dei poteri *ex* art. 218, ultimo comma, TFUE. A proposito della Corte, è sempre il caso di ricordare quella giurisprudenza che, in cause aventi ad oggetto "diritti digitali", ha portato a galla una serie di preoccupanti divergenze tra istituzioni su elementi cardine del sistema UE di tutela dei diritti fondamentali, fermo restando che queste pronunce non hanno avuto ricadute esclusivamente materiali o istituzionali, ma hanno riguardato le relazioni tra Unione e Stati terzi su profili salienti della *governance* del digitale. Tra gli esempi più lampanti si citano Corte giust. 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238 (con cui la Corte ha dichiarato l'invalidità integrale di un atto legislativo, ossia la direttiva sulla conservazione dei dati generati o trattati in relazione alla fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione), e 6 ottobre 2015, C-362/14, *Schrems*, ECLI:EU:C:2015:650 (nella fattispecie la Corte ha dichiarato l'invalidità di una decisione esecutiva della Commissione che in pratica certificava l'adeguatezza della protezione fornita dagli Stati Uniti ai dati personali trasferiti dagli Stati membri al rispettivo territorio).

strategia non fa mai menzione espressa della politica commerciale comune, Commissione e Alto Rappresentante dichiarano che «l'attuale panorama globale richiede forme di cooperazione nuove, più profonde e più flessibili al fine di promuovere partenariati reciprocamente vantaggiosi»[117]. Sicché, agli accordi di libero scambio o di associazione si dovrebbero affiancare non solo strumenti di aggiornamento in tema di commercio digitale e accordi *ad hoc* in questa materia: molti degli esempi di azioni future preventivate per ciascuna delle priorità suddette si riferiscono a partenariati, dialoghi e strumenti di natura finanziaria oppure operativa, segnatamente entro il perimetro della *Global Gateway*.

Da ultimo, e in linea di continuità con quanto appena esposto, non va trascurata la crescente portata dell'approccio securitario applicato all'evoluzione tecnologica, visibile nitidamente nella SDIUE. Nonostante i limiti in termini di attribuzioni disposti dall'art. 4, par. 2, TUE, è più che mai evidente il proseguimento del tentativo di ibridazione di competenze per il rafforzamento, mediante l'azione dell'Unione, della difesa e della sicurezza degli Stati membri[118]. C'è però da attendersi che gli Stati membri cercheranno di condizionare oltremodo simili "incursioni" nella dimensione esterna del MUD, in particolare tramite i propri rappresentanti in Consiglio. Anche se non ci si attende un diffuso ricorso a manovre di ostruzionismo, si ritiene plausibile che le principali regole di riferimento saranno (*rectius*, continueranno a maggior ragione ad essere) materialmente limitate e scarsamente prescrittive.

7. Conclusioni

Il nucleo dell'indagine che si è svolta si situava, come anticipato nell'introduzione, in seno a un quesito di fondo; ci si chiedeva in particolare quali fossero i tratti giuridici più evocativi dell'evoluzione della dimensione esterna del MUD. Ebbene, alla luce delle risultanze dell'analisi, e a caldo, verrebbe quasi da riformulare il quesito, domandandosi, casomai, se una (effettiva) dimensione esterna del MUD esista per davvero. In alternativa, si potrebbe essere indotti a ragionare sull'estensione territoriale di quegli atti legislativi che al contempo concorrono a dare corpo al MUD e, anche sulla scorta della giurisprudenza della Corte di giustizia, delineano tracce di "*Brussels effect*", nel tentativo

[117] COM(2025) 140 final, cit., p. 4

[118] F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited*, in *European Foreign Affairs Review*, 2023, p. 339.

di favorire un allineamento diretto o indiretto, ma pur sempre "dall'interno", delle condotte di soggetti pubblici e privati *extra*-UE rispetto alle regole e agli obiettivi fissati dall'Unione per il digitale[119].

Pur nella consapevolezza delle numerose variabili che limitano l'azione complessiva dell'Unione nell'attuale contesto internazionale (ma anche…europeo), ciò che emerge dallo studio realizzato è uno scenario nel quale gli accordi internazionali con cui l'Unione si prefigge di traslare al suo esterno i propri principi e obiettivi nell'ambito del commercio digitale sono limitati sotto vari punti di vista. I – più risalenti – capitoli sul commercio elettronico e quelli – più recenti – sul commercio digitale inclusi in certi ALS presentano un campo d'azione ristretto e, ancor più di frequente, una valenza tutt'altro che considerevole. Tale situazione non sembra poter essere messa in discussione dai nuovi partenariati digitali, né

[119] Si rinvia alla vasta dottrina sul tema, ad esempio: M. GÖMANN, *The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement,* in *Common Market Law Review*, 2017, p. 567 ss.; C. CELLERINO, *L'applicazione "territoriale" della normative UE in materia di protezione dei dati personali (GDPR) e l'economia globale dei dati: quale modello regolatorio?*, in G. GRECO, S. DOMINELLI (a cura di), *I mercati dei servizi tra regolazione e governance*, 2019, pp. 133 ss.; M. C. MENEGHETTI, *The Different Shapes of Extraterritoriality in EU Data Protection Law and its International Justifications,* in Diritto del commercio internazionale, 2019, p. 695 ss.; R. CAFARI PANICO, *Le imprese multinazionali, la protezione dei dati nello spazio cibernetico e l'efficacia extraterritoriale del diritto dell'Unione europea*, in *Papers di Diritto europeo*, 2021, p. 7 ss.; F. MARONGIU BONAIUTI, *L'ambito di applicazione territoriale del Digital Markets Act e del Digital Services Act. Tra applicazione "extraterritoriale" del diritto dell'Unione europea e attribuzione di un carattere internazionalmente imperativo alle sue norme*, in G. CAGGIANO, G. CONTALDI, P. MANZINI, *op. cit.,* p. 171 ss.; M. BURRI, K. KUGLER, *Regulatory Autonomy in Digital Trade Agreements,* in *Journal of International Economic Law*, 2024, p. 399; M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in *Eurojus*, 2024, p. 190 ss.; F. K, *A Constitutionally Oriented Reading of the EU Artificial Intelligence Act*, in L. MEZZETTI (a cura di), *Science, Technology and Law. Mutual Impact and Current Challenges,* Bologna, p. 229 ss.; H. DREWES, A. KIRK, *Extraterritorial Effects of the Digital Markets Act: The 'Elusive Long Arm' of European Digital Regulation,* in *World Competition*, 2024, p. 473 ss.; G. MONGA, *Data Act e diritto internazionale privato: continuità «unilateralista» e residui di «bilateralismo»,* in *SIDIBlog*, 26 agosto 2024; M. MÜLLER, M. C. KETTEMANN, *European Approaches to the Regulation of Digital Technologies*, in H. WERTHNER, C. GHEZZI, J. KRAMER, J. NIDA-RÜMELIN, B. NUSEIBEH, E. PREM, A. STANGER (a cura di), *Introduction to Digital Humanism. A Textbook*, Cham, 2024, p. 623 ss.; G. RUGANI, *La regolamentazione dei flussi di dati personali dall'UE verso Paesi terzi. Alla ricerca di un bilanciamento tra espansione del commercio internazionale e* personal data protection, Torino, 2024, p. 82 ss.; M. ŠONKOVÁ, *Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act* (EU Diplomacy Papers 4/2024), p. 1 ss.; G. STAZI, *Pluralismo e libertà nell'era dei tecnoligarchi: il ruolo dell'antitrust*, in C. SCHEPISI (a cura di), Unione europea, pluralismo e libertà dei media nell'era digitale, Napoli, 2025, p. 20.

dai pochissimi ACD che l'Unione ha concluso nell'ultimo biennio, a meno che non si voglia mettere in risalto l'ipotetica funzione preparatoria che questi strumenti potrebbero esercitare con riferimento a meccanismi di cooperazione che però al momento devono ancora essere immaginati.

E se mai si stessero creando le condizioni per un'intensificazione della proiezione dei pilastri del MUD all'esterno dell'Unione, pare che questo *trend* sia destinato a trovare terreno più fertile nelle relazioni con *partners* che tendenzialmente beneficiano di iniziative correlate alla politica UE di cooperazione allo sviluppo, come suggeriscono le novità che caratterizzano i rapporti UE-ACP. Detto altrimenti, la dimensione esterna del MUD potrebbe essere contraddistinta da un graduale distacco dalla PCC, che invece avrebbe dovuto rappresentare il terreno di sperimentazione privilegiato di questo processo, almeno stando agli intenti iniziali. Anzi, è addirittura verosimile che si stiano creando premesse aggiuntive per un freno al ricorso ad accordi internazionali, in luogo di iniziative di più incerta fisionomia, almeno se si assume la prospettiva del diritto dell'Unione. Se così fosse, l'azione dell'UE si porrebbe in maggiore controtendenza rispetto alle necessità reali che derivano dalla crisi sempre più profonda del multilateralismo e delle sue regole[120].

Infine, si ritiene che rimanga in sospeso un tema di primaria importanza, quale che sia la tipologia e la natura dello strumento o dell'iniziativa di volta in volta discusso: ci si riferisce alla protezione e alla promozione dei diritti fondamentali e dei valori comuni e fondanti dell'Unione, oltre che ai relativi profili di controllo. Il quadro restituito dal presente lavoro lascia altresì intendere che l'approccio antropocentrico che innerva la transizione digitale europea, ivi comprese le più pertinenti dinamiche di mercato, continua a non trovare riscontri tangibili nella dimensione esterna del MUD. Ancora non sta giungendo a maturazione quello stadio evolutivo più volte caldeggiato nella narrativa (assertiva) delle istituzioni UE e che presupporrebbe una "tensione valoriale" tale da riequilibrare logiche puramente commerciali e istanze di tutela e promozione dei diritti fondamentali e dei valori sovranazionali. Ne deriva

[120] In questo senso, F. NELLI FEROCI, *La crisi dell'integrazione europea*, in C. AMALFITANO, M. CONDINANZI (a cura di), *Paura dell'Europa: spunti di razionalizzazione*, Torino, 2020, p. 47. Si riporta anche l'opinione di chi annota che «while for the past two decades the Union has sought to pursue its objectives through multilateral cooperation in international organizations and through many partnerships with key actors, the concept of "strategic partnership" has remained underdeveloped». (J. WOUTERS, *The EU's Efforts to Uphold the International Rules-Based Order: Mission Impossible?,* in *Global Policy*, n. 8/2024, p. 79).

che propositi volti a determinare vere e proprie trasformazioni sistemiche dell'ordinamento dell'Unione, quali l'affermazione di un'autonomia strategica e di una sovranità tecnologica europee sul piano internazionale, rischiano in realtà di rivelarsi progetti largamente incompleti o, peggio ancora, incompiuti.

Sovranità digitale e *governance* globale: i profili giuridici delle politiche digitali nel mondo

di PAULINA KOWALICKA [*]

SOMMARIO: 1. La sovranità digitale: scenari internazionali. – 2. La *governance* digitale e le sfide etiche. – 3. Dalla nascita dell'intelligenza artificiale alle strategie moderne. – 4. Modelli normativi e politiche digitali: un'analisi comparata. – 4.1. L'approccio europeo. – 4.2. La prospettiva delle Americhe. – 4.3. I modelli *extra*-occidentali. – 5. Considerazioni conclusive.

1. La sovranità digitale: scenari internazionali

La digitalizzazione ha profondamente modificato i paradigmi tradizionali della sovranità, ponendo interrogativi fondamentali sulla capacità degli ordinamenti giuridici di esercitare un controllo effettivo sui flussi di dati, sulle infrastrutture digitali e sulle piattaforme tecnologiche[1]. Il concetto di "sovranità digitale" emerge come risposta a tale sfida, configurandosi come «la capacità di uno Stato o di un'entità sovranazionale di esercitare autonomia decisionale e controllo sulle proprie risorse digitali, infrastrutture e sui dati»[2]. Essa mira a garantire l'indipendenza e la sicurezza di una Nazione, proteggendo l'infrastruttura strategica e riducendo la dipendenza dai fornitori stranieri. In questo contesto, il concetto di sovranità digitale si intreccia con le dinamiche della *governance* digitale, rendendo necessaria una riflessione comparatistica sulle capacità dei diversi ordinamenti di affrontare la transizione tecnologica. In particolare, risulta fondamentale interrogarsi su quali siano le potenze globali che maggiormente stanno investendo nella trasformazione digitale, secondo una triplice prospettiva: quella finanziaria, relativa agli stanziamenti nella ricerca e nello sviluppo; quella normativa, concernente l'impegno regolatorio e la definizione di una efficace strategia di digitalizzazione; e, infine, quella sociale, afferente agli investimenti in alfabetizzazione digitale e *capacity building*.

[*] Assegnista di ricerca in informatica giuridica presso l'Università degli Studi di Milano.

[1] G. DE GREGORIO, *Digital constitutionalism in the new era of Internet governance*, in *International Journal of Law and Information Technology*, 2022, pp. 68-97.

[2] T. MADIEGA, *Digital sovereignty for Europe*, in *European Parliamentary Research Service*, 2020.

Il quadro globale della digitalizzazione risulta complesso: gli Stati Uniti dominano gli investimenti e la ricerca[3], la Cina si distingue per la rilevanza nel campo scientifico[4], i Paesi europei si affermano, invece, per l'alfabetizzazione digitale e l'impegno normativo. Se in precedenza lo scenario globale risultava polarizzato tra Stati Uniti e Cina, con l'Unione europea relegata a un ruolo marginale, attualmente si assiste a una progressiva riconfigurazione degli equilibri globali. Come si avrà modo di vedere nei paragrafi successivi, Paesi come l'India, il continente africano, alcune Nazioni dell'America latina stanno assumendo un ruolo sempre più rilevante nello sviluppo e nella regolazione delle nuove tecnologie, contribuendo, in questo modo, all'espansione dell'ecosistema digitale globale.

2. La *governance* digitale e le sfide etiche

La rapida affermazione di tecnologie emergenti, che fungono da pilastro di una nuova economia digitale trasformatasi presto in capitalismo, si impone come realtà dominante, entrando in conflitto con l'aspettativa che il diritto – nella sua espressione più alta, quella dei diritti umani e della ricerca del "giusto" o dell'"etico" – possa prevalere in quelle aree così delicate e suscettibili al progresso, e di conseguenza, così mutevoli e inclini al rischio. Da un lato, termini come dignità, uguaglianza, libertà, giustizia compaiono in maniera ridondante in ogni piano d'azione politico, economico e finanziario; d'altro canto, sembrano quasi essere estranei al linguaggio collettivo, in una realtà sempre più dominata da un evidente squilibrio tra i semplici utenti o consumatori e i grandi investitori del digitale[5].

In tale processo, l'Unione europea si è dimostrata reattiva nel delineare le politiche digitali, che comprendano i temi dell'affidabilità, dell'inclusione digitale e della sostenibilità. Questi valori sono alla base di una strategia politica e regolamentare ambiziosa, volta a promuovere una transizione tecnologica che sia etica, equa nell'accesso e fondata sulla fiducia dei cittadini. I diritti e i valori dell'UE, infatti, sono al centro

[3] Secondo i dati dell'*AI Index Report* – Stanford University, Human-Centered Artificial Intelligence – del 2025, gli Stati Uniti hanno investito circa cinquecento miliardi di dollari in ricerca e sviluppo.

[4] Secondo i dati dell'Organizzazione mondiale della Proprietà Intellettuale (WIPO) tra il 2014 e il 2023 la Cina ha depositato più di trentotto mila brevetti in ambito IA. Per un approfondimento, si consulti il sito: https://www.wipo.int/portal/en/index.html.

[5] L. AVITABILE, *Diritti umani e IA*, in A. LALLI (a cura di), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Torino, 2024.

dell'approccio al digitale, definito *human-centered*, in una prospettiva di equilibrio tra la Cina, fortemente sbilanciata sul centralismo dello Stato e l'America, considerata eccessivamente *business-friendly.*

L'adozione crescente di tecnologie basate sull'intelligenza artificiale solleva questioni complesse, non solo dal punto di vista tecnico, ma anche sotto il profilo etico e giuridico. Le preoccupazioni etiche rappresentano, probabilmente, una delle ragioni principali per cui i responsabili politici si sono occupati – e continuano a occuparsi – della rivoluzione tecnologica e delle politiche digitali[6]. La *governance* etica delle tecnologie digitali, infatti, non è solo una questione normativa, ma anche un tema sociale e politico di grande rilevanza[7].

3. Dalla nascita dell'intelligenza artificiale alle strategie moderne

Le prime tracce di intelligenza artificiale come disciplina scientifica risalgono agli anni Cinquanta e, nonostante siano trascorsi più di settant'anni, ancora oggi, le teorie e definizioni di intelligenza artificiale più convincenti e accettate sono quelle proposte da Alan Turing o da McCarthy, Minsky, Rochester e Shannon. Proprio nel 1950 il matematico scrisse un articolo in cui proponeva quello che sarebbe divenuto noto come il test di Turing[8], non verificando se una macchina possa pensare come un essere umano ma se sia in grado di simulare il comportamento intelligente umano al punto da non essere riconosciuta come artificiale. Nel 1955 gli studiosi nella loro "Proposta per il progetto estivo di ricerca sull'intelligenza artificiale di Dartmouth" hanno gettato le fondamenta dei primi studi sul tema: «il problema dell'intelligenza artificiale è quello di far sì che una macchina agisca con modalità che sarebbero definite intelligenti se un essere umano si comportasse allo stesso modo»[9], di fatto distinguendo i concetti di "agire" e "intelligenza".

---

[6] A titolo esemplificativo, si pensi al tema della *privacy*, che ha avuto le conseguenze più visibili nella politica e nel diritto. La *privacy* come questione etica avente implicazioni giuridiche può essere fatta risalire al XIX secolo con Warren e Brandeis, e i conseguenti principi, giuridicamente vincolanti, hanno assunto particolare rilievo già a partire dagli anni '70 fino a definire una vera e propria legislazione formale sulla protezione dei dati a partire dagli anni '80.

[7] Si veda, L. FLORIDI, J. COWLS, M. BELTRAMETTI ET AL., *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds & Machines*, 2018, pp. 689-707.

[8] A. TURING, *Computing machinery and intelligence*, in *Mind*, 1950, pp. 433-460.

[9] J. MCCARTHY, M.L. MINSKY, N. ROCHESTER, C.E. SHANNON, *A proposal for the Dartmouth summer research project on artificial intelligence,* in *AI Magazine*, 1955 (riedizione 2006); L. FLORIDI, *Etica dell'intelligenza artificiale, Sviluppi, opportunità, sfide*, Milano, 2022.

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale[10], all'art. 3, propone una definizione molto scarna; infatti, un sistema di intelligenza artificiale viene definito come: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input, che riceve, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

In un sistema di intelligenza artificiale, il vero successo non riguarda la "produzione", bensì la sostituzione dell'intelligenza umana (anche in termini di efficacia)[11] per raggiungere un risultato o per eseguire un numero elevato di attività che richiederebbero l'intervento umano. L'intelligenza artificiale, dunque, sembra non costituire tanto il risultato della creazione di macchine davvero intelligenti, quanto il prodotto di una progressiva costruzione di un ecosistema digitale che ne facilita il funzionamento. Si tratta di un universo in cui la logica matematica ha progressivamente lasciato spazio ai modelli statistici, i dati hanno registrato una crescita esponenziale e gli algoritmi operano attraverso correlazioni probabilistiche.

L'intelligenza artificiale e i dati, dunque, si intrecciano in maniera diretta con il concetto di sovranità digitale proprio perché i dati rappresentano l'elemento chiave dello sviluppo delle nuove tecnologie[12]. Nella società, ormai sempre più interconnessa, numerosi ambiti fondamentali – tra cui la sanità, la finanza, la robotica, il mondo del lavoro e, perfino, il sistema giudiziario – sono profondamente trasformati dall'enorme quantità di dati generati, raccolti e analizzati in tempo reale. Questi dati, resi leggibili e interpretabili da sistemi digitali, alimentano algoritmi e intelligenze artificiali capaci di automatizzare decisioni e processi che un tempo richiedevano l'intervento umano. Le macchine, grazie a *software* avanzati e modelli predittivi, non si limitano più a eseguire semplici comandi, ma sono in grado di adattarsi a situazioni

[10] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in *GUUE* L 2024/1689 del 12 luglio 2024.

[11] L. FLORIDI, *Etica dell'intelligenza artificiale, Sviluppi, opportunità, sfide*, Milano, 2022.

[12] S. FRATINI, E. HINE, C. NOVELLI ET AL., *Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models*, in *DISO*, 2024.

complesse, ottimizzare risorse e agire con efficienza e rapidità. Come osserva lo studioso Floridi, il punto cruciale risulta evidente: tali sistemi presentano, evidentemente, una "intelligenza zero", nel senso che non possiedono capacità cognitive autonome; tuttavia, conseguono risultati straordinari poiché gli esseri umani hanno progressivamente modificato gli ambienti e le infrastrutture tecnologiche, in modo da renderli compatibili con le capacità computazionali degli algoritmi. Le prestazioni di tali tecnologie, dunque, derivano dall'adeguamento del contesto digitale, dalla disponibilità massiva dei dati e dall'implementazione dei sistemi che consentono agli algoritmi di funzionare con efficienza e precisione.

Questo scenario apre innumerevoli opportunità, ma solleva anche interrogativi etici, sociali e legali sull'affidabilità delle decisioni automatizzate e sul ruolo dell'essere umano in un mondo guidato sempre più da logiche algoritmiche. Tra le questioni emergenti si evidenziano, tra le altre, l'autonomia decisionale delle macchine e i suoi limiti; il rischio di perpetuazione e amplificazione dei *bias* insiti nei dati e negli algoritmi; l'esigenza di esplicabilità (intesa come la capacità di rendere comprensibili i processi decisionali automatizzati); nonché i principi di equità, tutela della *privacy*, tracciabilità della responsabilità, trasparenza e costruzione della fiducia nei confronti delle tecnologie.

Tali problematiche impongono una riflessione critica sull'adeguatezza degli attuali strumenti normativi e sulla necessità di sviluppare nuove politiche e cornici legislative capaci di governare l'interazione tra i sistemi intelligenti e i diritti fondamentali, nel rispetto della dignità e dell'autodeterminazione umana.

4. Modelli normativi e politiche digitali: un'analisi comparata

4.1. L'approccio europeo

In Europa, come detto in apertura, l'approccio si fonda su una visione umano centrica e precauzionale dell'innovazione. L'Unione europea ha dimostrato una spiccata capacità di reazione e visione strategica nella definizione delle proprie politiche digitali, articolando un insieme coerente di interventi normativi e programmatici orientati alla salvaguardia dei diritti umani, ai principi di affidabilità tecnologica, inclusione digitale e sostenibilità ambientale. Tali valori costituiscono il fondamento di una politica digitale ambiziosa, che mira non solo a promuovere l'innovazione, ma anche a guidare la transizione tecnologica in settori fondamentali, secondo i criteri di equità, eticità e tutela della fiducia. La prospettiva delineata si proietta verso un obiettivo di lungo termine: la costruzione di

un ecosistema digitale avanzato, resiliente e sostenibile, che possa concorrere anche al raggiungimento della neutralità climatica entro il 2050. In tale contesto, le tecnologie digitali sono intese come strumenti funzionali non solo alla competitività economica, ma anche al miglioramento del benessere collettivo.

Al centro del cosiddetto "decennio digitale" europeo si colloca l'impegno a sviluppare e rafforzare cinque aree strategiche: il potenziamento dell'infrastruttura informatica, la valorizzazione dei dati, lo sviluppo di algoritmi e tecnologie avanzate, la semplificazione delle regole e la promozione delle competenze digitali nella popolazione[13]. Tali ambiti sono considerati essenziali per assicurare l'autonomia strategica dell'Unione europea nel contesto globale, riducendo la dipendenza da attori extraeuropei e affermando una sovranità digitale basata sul rispetto dei diritti fondamentali e dei valori democratici. La strategia europea in materia digitale si configura, dunque, come una risposta normativa ed economica integrata, orientata a un utilizzo dei dati che sia efficiente, trasparente, affidabile e conforme al carattere giuridico.

L'Unione europea ha delineato un quadro normativo articolato, fondato sul rischio, che mira a garantire la conformità dei sistemi di IA ai principi di trasparenza, equità, sicurezza e responsabilità. Nel contesto geopolitico, la strategia dell'Unione europea si presenta come leader nel campo della regolamentazione, con l'intento di affermare la propria sovranità digitale e rappresentare uno standard globale, adottabile in altre parti del mondo – il cosiddetto "effetto Bruxelles"[14].

In passato, l'UE ha dimostrato una capacità distintiva tra gli attori internazionali di promulgare regolamenti in grado di plasmare il contesto economico e imprenditoriale globale, elevando gli standard in tutto il mondo e determinando una significativa europeizzazione di molteplici aspetti rilevanti. Anche con riferimento alla transizione digitale, l'Unione ha tentato di porsi, ad esempio con il Regolamento sull'intelligenza artificiale, come punto di riferimento, influendo su tante attività regolatorie ed esercitando – indirettamente – una profonda influenza sul comportamento delle aziende e sulle relazioni internazionali[15]. Tuttavia,

[13] Commissione europea, *AI Continent Action Plan*, 2025. Per un approfondimento consultare il sito: https://digital-strategy.ec.europa.eu/en/factpages/ai-continent-action-plan.
[14] A. BRADFORD, *The Brussels effect: how the European Union rules the world*, New York, 2020.
[15] A. BRADFORD, *op. cit*.

come sottolineato anche dallo studioso Floridi, tale effetto si rivela particolarmente efficace nei settori connessi ai prodotti fisici o analogici, mentre risulta essere limitato nell'ambito digitale. In tale contesto, la legislazione europea sembra comunque generare un effetto – che può essere qualificato come *template effect* – in virtù del quale l'Europa funge da precursore normativo, offrendo un modello suscettibile di essere adattato e migliorato da altri ordinamenti, senza però esportare in maniera (pressoché) automatica i propri standard normativi.

Occorre, inoltre, rilevare che l'eccessiva regolamentazione, in particolare in settori come l'intelligenza artificiale e le nuove tecnologie, rischia di frenare l'innovazione e di compromettere la competitività delle imprese europee rispetto ai concorrenti internazionali. Un quadro normativo eccessivamente stringente e frammentato, infatti, rischia di penalizzare l'iniziativa privata, scoraggiare gli investimenti in ricerca e sviluppo e rallentare la crescita economica.

Il sempre crescente impatto di tali tecnologie sulla società, sulla democrazia, sulla sovranità ha spinto le istituzioni europee – insieme ad altri attori internazionali – a intensificare i propri sforzi normativi, nel tentativo di governare la transizione digitale e mitigare i possibili rischi. In questo contesto, il tema del rapporto tra IA e diritti umani si impone come uno degli snodi centrali del dibattito politico e giuridico contemporaneo, ancora ampiamente aperto e soggetto a evoluzioni rapide e complesse. A livello europeo, negli anni, sono emerse numerose iniziative orientate non solo alla regolamentazione vincolante, ma anche alla promozione di strumenti di *soft law*, come linee guida, raccomandazioni e codici etici, che mirano a orientare l'uso dell'IA in una direzione responsabile e rispettosa dei valori fondamentali. Questi interventi, pur differenziandosi per forma e intensità, condividono una visione comune: quella di un ecosistema digitale costruito attorno alla centralità dell'essere umano.

Il Regolamento sull'intelligenza artificiale, entrato in vigore il 1° agosto 2024, rappresenta un vettore fondamentale per la creazione di un quadro normativo solido e armonizzato in materia di IA, che affronta i rischi e posiziona l'Europa a svolgere un ruolo di guida a livello mondiale. Gli obiettivi del regolamento sono migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme, in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale, promuovere la diffusione di un'intelligenza artificiale antropocentrica e affidabile, garantendo nel

contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, e proteggere contro gli effetti nocivi dei sistemi di IA. Il presente quadro normativo garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del regolamento stesso.

Il Regolamento sull'intelligenza artificiale, inserendosi in un più ampio e articolato quadro normativo sulle nuove tecnologie, contribuisce a definire la sovranità digitale europea, incentrata su una prospettiva umano centrica, in un contesto globale complesso e spesso orientato da priorità differenti.

4.2. La prospettiva delle Americhe

Gli Stati Uniti hanno scelto, invece, un percorso diverso, perseguendo un approccio decentralizzato alla regolamentazione dell'intelligenza artificiale. Il paradigma statunitense è tradizionalmente caratterizzato da una politica orientata al mercato e incentrata sulla libertà di espressione quale valore costituzionale primario tutelato dal Primo Emendamento, che può essere considerato, quest'ultimo, la legittimazione costituzionale delle piattaforme digitali e, allo stesso tempo, una barriera contro l'intervento normativo[16]. La strategia americana ha storicamente privilegiato una filosofia regolatoria maggiormente liberale, fondata su un sistema collaborativo fra agenzie governative e multinazionali digitali, riconoscendo alle imprese private ampi margini di autodeterminazione e azione, con i rischi, talvolta, di compromettere la coerenza regolatoria e amplificare la frammentazione normativa[17]. Tale modello si inserisce nel più ampio contesto della tradizione statunitense della co-regolazione e dell'uso di strumenti non vincolanti, come linee guida, standard tecnici, *policy*, *best practices* che, pur garantendo flessibilità e ampio margine di

[16] G. DE GREGORI, *Digital constitutionalism across the Atlantic*, in *Cambridge University Press*, 2022; E. CHEMERINSKY, *Constitutional Law: Principles and Policies*, Wolters Kluwer, 2019. Per un approfondimento, si veda Human Centered Artificial Intelligence, Stanford University *The 2025 AI Index Report,* 2025. Per un'ulteriore analisi, si consulti il sito: https://hai.stanford.edu/ai-index/2025-ai-index-report.
[17] R.A. POSNER, *Economic analysis of law*, Wolters Kluwer, 2007 (VII Ed.).

adattamento all'innovazione tecnologica, presenta significative lacune in termini di responsabilità e tutela dei diritti fondamentali.

L'assenza di una legislazione uniforme sull'intelligenza artificiale, spesso, alimenta l'errato sospetto che gli Stati Uniti non abbiano intrapreso azioni sostanziali sull'intelligenza artificiale e sull'implementazione delle nuove tecnologie. Il programma di sviluppo dell'IA, in realtà, ha avuto inizio nel 2016, durante la Presidenza di Barack Obama, con la pubblicazione della prima versione del *National Artificial Intelligence Research and Development Strategic Plan*, segnando la prima di tre fasi della politica digitale americana, che corrispondono ai tre distinti cicli amministrativi, con un progressivo orientamento alla minimizzazione dell'intervento governativo e al rafforzamento del concetto di "capitalismo di libero mercato"[18]. Il Congresso ha fino ad ora evitato un quadro normativo unitario, concentrandosi, invece, su numerosi interventi settoriali[19] per gestire i molteplici rischi e le opportunità derivanti da una rapida accelerazione dello sviluppo. Tali iniziative includono la regolamentazione dei sistemi ad alto rischio, l'introduzione di requisiti di valutazione e trasparenza, la definizione di un'autorità di vigilanza normativa e la protezione dei consumatori attraverso strumenti di responsabilità[20]. L'obiettivo strategico di tale approccio è duplice: da un lato, mitigare i potenziali rischi legati all'adozione di sistemi di intelligenza artificiale; dall'altro, garantire la *leadership* degli Stati Uniti nella ricerca, nello sviluppo e nell'implementazione delle nuove tecnologie. Tra gli interventi normativi più significativi, configura il *National AI Initiative Act,* del 2020, che ha istituito un Ufficio responsabile della supervisione e dell'attuazione delle nuove tecnologie, e il *Blue Print for an AI Bill of Rights*, che ha rappresentato uno dei progetti più rilevanti dell'amministrazione del Presidente Biden, delineando linee guida per l'accesso e l'utilizzo equo dei sistemi di IA attraverso cinque principi, e le

[18] E. HINE, L. FLORIDI, *Artificial intelligence with American values and Chinese characteristics: a comparative analysis of American and Chinese governmental AI policies,* in *AI & Society,* 2024, pp. 257-278.

[19] Per un approfondimento sulle iniziative di legge promulgate, in attesa o fallite, si consultino i seguenti siti: https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation, https://www.bclplaw.com/en-US/events-insights-news/us-state-by-state-artificial-intelligence-legislation-snapshot.html.

[20] S. PARINANDI, J. CROSSON, K. PETERSON, S. NADAREVIC, *Investigating the politics and content of US State artificial intelligence legislation*, in *Cambridge University Press*, 2024.

relative pratiche, per guidare la progettazione, l'uso e l'implementazione di sistemi automatizzati, tra cui sistemi sicuri ed efficaci; discriminazione e protezione algoritmica; riservatezza dei dati; notifica e spiegazione; alternative umane, considerazioni e *fallback*. La complessità del quadro regolatorio statunitense si è accentuata durante l'amministrazione Trump, caratterizzandosi ulteriormente per una precisa strategia orientata al primato dell'innovazione sulla regolamentazione. Nel gennaio 2025, il Presidente ha firmato l'ordine esecutivo *Removing Barriers to American Leadership in Artificial Intelligence* segnando un punto di svolta e revocando l'approccio regolatorio dell'amministrazione precedente[21]. Successivamente, nel luglio 2025, il governo americano ha articolato una nuova strategia politica – *AI Action Plan* – fondata sulla rimozione delle barriere normative, sulla accelerazione dell'innovazione, attraverso investimenti nella ricerca e nello sviluppo delle infrastrutture, e sulla formazione del capitale umano, mediante un significativo programma di alfabetizzazione[22].

Tali azioni stanno, evidentemente, riconfigurando l'impianto regolatorio incidendo sul rapporto tra la responsabilità del settore pubblico e il controllo federale centralizzato nell'ecosistema tecnologico, stimolando sempre di più il dibattito sulla flessibilità del governo federale e sulla coerenza normativa nazionale, imponendo un – inevitabile – bilanciamento tra centralizzazione e autonomia locale.

La regione sudamericana, d'altro canto, si caratterizza per significative diseguaglianze economiche, politiche e sociali e una marcata eterogeneità nello sviluppo tecnologico. Alcuni Paesi hanno intrapreso, negli ultimi anni, percorsi di investimento nelle infrastrutture e nei processi di digitalizzazione, mentre altri faticano a colmare le carenze strutturali che si manifestano a livello infrastrutturale, formativo, finanziario e politico-sociale. In tale contesto, la dipendenza da attori stranieri costituisce un elemento di vulnerabilità, poiché limita la capacità dei governi di esercitare un controllo effettivo sui propri dati, sulle reti e, in generale, sulla sovranità digitale. Una delle principali criticità risiede nell'instabilità politica e istituzionale, alla quale si associa la limitata

[21] Executive Order 14110 del 30 ottobre 2023, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* disponibile al seguente indirizzo *Internet*: www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf.

[22] Per un approfondimento si consulti il testo America's AI Action Plan al sito: https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

disponibilità di risorse destinate alla ricerca e allo sviluppo. La complessità culturale ed economica della regione ostacola l'adozione di un approccio normativo uniforme in materia di intelligenza artificiale: ogni Paese presenta priorità differenti, complicando il processo di elaborazione di standard condivisi, sebbene stia progressivamente emergendo una crescente consapevolezze circa la necessità di sviluppare forme di sovranità tecnologica, potenziando la capacità di definire delle politiche digitali autonome ed efficienti[23].

In particolare, Brasile, Cile, Argentina, Messico e Colombia risultano tra gli ordinamenti più attivi nell'attuazione delle politiche digitali e nel rafforzamento dell'infrastruttura. Al contrario, i Paesi con minor sviluppo affrontano gravi limitazioni strutturali, come la bassa connettività, un'alfabetizzazione limitata, la dipendenza dalle tecnologie straniere, incidendo negativamente sulla competitività e sulla capacità di innovazione[24]. Sta emergendo, infatti, una crescente consapevolezze della necessità di sviluppare, anche in questi Paesi, forme di sovranità tecnologica, potenziando la capacità di definire delle politiche digitali efficienti. Diversi Paesi stanno investendo non solo nell'elaborazione di linee guida etiche, ma soprattutto nella definizione di quadri normativi e politiche di alfabetizzazione, sollevando, tuttavia, preoccupazioni circa l'inadeguatezza dei processi decisionali[25].

Tra gli ordinamenti più dinamici, si distinguono il Brasile e il Cile. Il 10 dicembre 2024, il Brasile ha approvato il disegno di legge 2338/2023, destinato a costituire il primo quadro normativo in materia di IA, inserendosi in un progetto più ampio che mira a coniugare lo sviluppo delle tecnologie con la tutela dei diritti e adottando un approccio basato sul rischio ispirato, in parte, al modello europeo. La regolamentazione brasiliana rappresenta, dunque, un tentativo di rafforzare la sovranità

[23] M.L. FLÓREZ ROJAS, *The Shaping of AI Policies in Latin America: A Study of International Influence and Local Realities*, in J. GOOSSENS, E. KEYMOLEN, A. STANOJEVIĆ (a cura di), *Public Governance and Emerging Technologies*, Springer, 2025.
[24] D.P.C. GALVEZ, S. REVINOVA, *Assessing Digital Technology Development in Latin American Countries: Challenges, Drivers and Future Directions*, in *MDPI Journals*, 2025. Per una panoramica completa, si veda: Oxford Insights, *Government AI Readiness Index,* 2024.
[25] M.L. FLÓREZ ROJAS, *The Shaping of AI Policies in Latin America: A Study of International Influence and Local Realities*, in J. GOOSSENS, E. KEYMOLEN, A. STANOJEVIĆ (a cura di), *Public Governance and Emerging Technologies*, Springer, 2025. Per un approfondimento si veda: L. BELLI, W.B. GASPAR, S.S. JASWANT, *Data Sovereignty and Data Transfers as Fundamental Elements of Digital Transformation: Lessons from the BRICS Countries*, in *Computer Law & Security Review*, 2024.

nazionale, riducendo la dipendenza da standard normativi stranieri, pur ispirandosi all'approccio europeo[26] e si propone come modello in grado di influenzare altri ordinamenti latinoamericani nel delineare la *governance* dell'IA. Analogamente, il Cile ha adottato, nel 2021, la Politica nazionale sull'IA, aggiornata nel 2023, fondata su tre pilastri: i fattori abilitanti, quali infrastrutture, risorse umane e dati; lo sviluppo e la ricerca; la governance e l'etica.

Nel 2024 è stato presentato un disegno di legge specifico sull'intelligenza artificiale, ispirato alle raccomandazioni UNESCO del 2021[27], con l'obiettivo di integrare i principi di trasparenza, *accountability* e tutela dei diritti fondamentali, realizzando, così, un modello ibrido che combina elementi di autoregolamentazione e valori europei, con un'attenzione particolare all'ecosistema locale e alle *startup*[28]. I modelli brasiliano e cileno dimostrano come l'America Latina stia cercando di collocarsi attivamente nella *governance* globale dell'IA, sperimentando degli approcci politici e regolatori, che pur ispirati ai principi europei, si adattano alle specificità e priorità locali.

4.3. I modelli *extra*-occidentali

Negli ultimi decenni la Cina, forte della più ampia base di utenti Internet al mondo[29], si è affermata come una superpotenza emergente, in crescente collisione con gli Stati Uniti, ritrovandosi coinvolta in un'intensa competizione geopolitica ed economica, in grado di influenzare in maniera significativa l'assetto dei mercati internazionali[30]. Il modello di *governance* cinese si colloca all'estremo opposto rispetto alla filosofia liberale occidentale: la Repubblica Popolare Cinese, infatti, rappresenta l'archetipo di un sistema politico fortemente centralizzato, pianificato e orientato al lungo termine, in cui lo Stato assume un ruolo di supervisione e guida sia nella definizione degli obiettivi che nell'impiego delle risorse. Tale configurazione trova il proprio fondamento giuridico nell'art. 1 della

[26] A. FRAZÃO, *Regulation of artificial intelligence in Brazil: examination of Draft Bill no. 2338/2023*, in *UNIO – EU Law Journal*, 2024.
[27] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021.
[28] UNESCO, *Chile: Artificial Intelligence Readiness Assessment Report*, 2024.
[29] Per un approfondimento si consulti il sito: https://english.www.gov.cn/archive/statistics/202507/21/content_WS687dd259c6d0868f4e8f4501.html.
[30] D. ZHANG, *Understanding the evolution of China's approach to digital trade: interests, ideas, and institutions*, in *ARPE*, 2024; M. JIANG, *Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa*, in *P&I*, 2024.

Costituzione della Repubblica Popolare Cinese del 1982, con l'ultima revisione nel 2018, che definisce la Cina come «Stato socialista sotto la dittatura democratica popolare» e sancisce il ruolo guida del Partito Comunista Cinese, elevando il pensiero di Xi Jinping a principio costituzionale vincolante[31]. L'architettura costituzionale cinese, caratterizzata dal principio del "centralismo democratico", previsto all'art. 3 della Costituzione, legittima un sistema in cui le tecnologie digitali avanzate vengono impiegate come strumento di controllo politico, sorveglianza e propaganda di Stato[32].

Da quando Xi Jinping è salito al potere nel 2012, l'obiettivo è diventato quello di sfruttare il mercato globale per potenziare la sua economia e guidare la riforma del sistema di *governance* globale[33], individuando l'IA come strumento fondamentale per la trasformazione economica, la videosorveglianza di massa, il rafforzamento della sicurezza nazionale e l'accrescimento della propria influenza geopolitica. Tale orientamento strategico si è concretizzato nel XIII Piano Quinquennale (2016-2020) che ha elevato l'innovazione tecnologica a priorità nazionale e nel XIV Piano Quinquennale (2021-2025) che considera l'intelligenza artificiale essenziale per il conseguimento degli obiettivi di modernizzazione socialista[34].

A partire dal *New Generation Artificial Intelligence Development Plan* del 2017, la Cina ha dimostrato un forte interesse nel plasmare l'emergente ordine globale dell'intelligenza artificiale, attraverso una serie di politiche e azioni concrete, con lo scopo di definire un sistema normativo etico e con l'ambizione di diventare la superpotenza globale dell'IA entro il 2030. Pubblicato dal Consiglio di Stato, tale Piano funge da documento unificato che delinea gli obiettivi della politica di intelligenza artificiale della Cina, fornendo l'indicazione più trasparente e influente delle forze trainanti alla base della strategia relativa

---

[31] L.C. BACKER, *The Communist Party as Polity and the Chinese Party-State Constitutional Order*, in N.S. BUI, S. HARGREAVES, R. MITCHEL (a cura di), *Handbook of Constitutional Law in Greater China*, Routledge, 2022.

[32] S. FELDSTEIN, T*he Rise of Digital Repression: How Technology is Reshaping Power, Politics and Resistance*, in *Oxford University Press*, 2022.

[33] J. CHENG, J. ZENG, *Shaping AI's Future? China in Global AI Governance*, in *Journal of Contemporary China*, 2022, pp. 794-810.

[34] National Development and Reform Commission, *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035, 2021.*

all'intelligenza artificiale del Paese[35]. Il governo di Pechino, ad agosto 2025, ha ultimato l'iniziativa *AI Plus*, la strategia più ambiziosa e mai elaborata dalla Cina per integrare l'intelligenza artificiale in ogni ambito e consolidarne il ruolo come motore della crescita futura[36]. Tale iniziativa si configura come una direttiva intersettoriale che impone l'integrazione dell'IA in diversi settori, tra cui la manifattura, l'agricoltura, la sanità, l'istruzione, i trasporti, la pubblica amministrazione.

Il modello cinese si fonda su un'integrazione tra settore pubblico e privato, in cui le principali aziende tecnologiche – Baidu, Alibaba, Tencent –, le università e gli enti di ricerca operano in stretta connessione con le istituzioni statali. Questa cooperazione, tuttavia, si configura entro un perimetro di autonomia limitata, poiché le aziende – pur dotate di risorse economiche rilevanti – rimangono subordinate all'orientamento e alle priorità di rilevanza politica e nazionale. La Legge sulla sicurezza nazionale del 2015 (*National Security Law*) impone, infatti, a tutte le organizzazioni e ai cittadini il dovere di sostenere, assistere e cooperare con le attività di sicurezza nazionale, configurando un obbligo giuridico vincolante che limita strutturalmente l'autonomia imprenditoriale. Tale vincolo è stato ulteriormente rafforzato dalla Legge sull'intelligence nazionale del 2017 (*National Intelligence Law*), che stabilisce che «qualsiasi organizzazione o cittadino deve sostenere, assistere e cooperare con il lavoro di intelligence nazionale» imponendo, di fatto, alle aziende di fornire dati e strumenti, alle autorità statali, su richiesta e senza possibilità di opporsi, evidenziando, in questo modo, delle incompatibilità con gli standard internazionali in materia di protezione dei dati personali.

L'intelligenza artificiale rappresenta uno strumento di crescita economica e competitività, nonché l'infrastruttura strategica in grado di rafforzare la stabilità sociale, garantire l'ordine politico e consolidare il controllo ideologico. Il governo cinese ha, infatti, ideato il Sistema di credito sociale, un meccanismo di valutazione sociale su base algoritmica previsto dal Piano di costruzione del sistema di credito sociale (2014-2020), che assegna punteggi a cittadini e imprese sulla base del

[35] H. ROBERTS, J. COWLS, J. MORLEY, ET AL., *The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation*, in *AI & Society*, 2021; A. BAZAVAN, C.E. HUIDUMAC-PETRESCU, *China's Drive for Technological Leadership, in Artificial Intelligence. Key Policies and Government-Industry Integration*, in M. BUSU (a cura di) *Digital Economy and the Green Revolution*, Spinger, 2023.

[36] Per un approfondimento si veda: The State Council the people's Republic of China, *China issues guideline to accelerate 'AI Plus' integration across key sectors*, 2025.

comportamento sociale, economico e politico, con conseguenze dirette sull'accesso a servizi pubblici. Tale sistema configura una forma di "*governance* algoritmica" che estende il controllo statale oltre i confini tradizionali del diritto penale o amministrativo, creando un nesso tra la condotta legale e quella socialmente disapprovata[37].

A partire dal 2020 il Paese ha intrapreso un percorso normativo volto alla definizione di standard giuridici ed etici nell'ambito dell'uso dell'intelligenza artificiale e della protezione dei dati personali[38], con una duplice logica. Da un lato, colmare il divario regolatorio con gli ordinamenti democratici occidentali, soprattutto quello europeo; dall'altro, assicurare che la disciplina giuridica non ostacoli, anzi potenzi, la capacità dello Stato di servirsi di tale tecnologia.

Il quadro normativo cinese si articola su più livelli gerarchici. Innanzitutto, la Legge sulla protezione delle informazioni personali (PIPL), entrata in vigore il 1° novembre 2021, rappresenta il primo quadro regolatorio sulla protezione dei dati in Cina, ispirato al modello europeo del GDPR, del quale replica numerosi istituti. Tuttavia, il PIPL si distingue significativamente dal quadro europeo sotto diversi profili sostanziali, ad esempio l'art. 13 prevede che il trattamento sia lecito anche quando «necessario per adempiere ai doveri statutari o agli obblighi legali», formulazione ampia che legittima estese deroghe in nome della sicurezza nazionale e dell'ordine pubblico; l'art. 38 introduce regole stringenti per il trasferimento transfrontaliero di dati, imponendo valutazioni di sicurezza governative per i processori di informazioni personali; l'art. 51 riconosce esplicitamente la sovranità, la sicurezza e gli interessi di sviluppo nazionali come limiti alla protezione dei dati personali[39].

La Legge sulla sicurezza dei dati (DSL), entrata in vigore il 1° settembre 2021, classifica i dati in base alla loro rilevanza per la sicurezza nazionale e l'interesse pubblico, imponendo obblighi di protezione e controllo statale.

Per quanto concerne, nel dettaglio, l'intelligenza artificiale, la Cina ha emanato una serie di regolamenti settoriali, tra cui le *Provisions on the*

[37] X. DAI, *Toward a Reputation State: The Social Credit System Project of China*, 2018.
[38] Si pensi, a titolo esemplificativo, alla Legge sulla protezione delle informazioni personali della Repubblica Popolare (PIPL, 2021), Legge sulla sicurezza dei dati (DSL, 2021), Legge sul deepfake (2023). Per un approfondimento, si veda M. SHEEHAN, *China's AI Regulations and How They Get Made*, in *Journal of International Relations and Sustainable Development*, 2023.
[39] R. CREEMERS, *China's Emerging Data Protection Framework*, in *Journal of Cybersecurity*, 2022.

Administration of Algorithmic Recommendations in Internet Information Services del 2022 che impongono trasparenza e la possibilità, per gli utenti, di disattivare i sistemi di raccomandazione algoritmica, ma richiedono anche l'utilizzo in conformità ai valori socialisti fondamentali; le *Provisions on the Management of Deep Synthesis Internet Information Services* (Legge sul *deepfake*) del 2023 che introduce obblighi di etichettatura e rigidi meccanismi di responsabilità, vietando usi che minaccino l'unità nazionale o l'immagine dello Stato; le *Interim Measures for the Management of Generative Artificial Intelligence* del 2023 sull'IA generative che richiedono dataset conformi ai valori socialisti e il controllo dei contenuti generati; le *Provisions on Promoting and Regulating Cross-border Data Flows* del 2024 che facilitano il trasferimento transfrontaliero di dati attraverso procedure standardizzate.

Tale sistema normativo, dunque, riflette la struttura costituzionale autoritaria del Paese, servendo, principalmente, al controllo politico e sociale, nonostante richiami formalmente la tutela dei diritti fondamentali secondo il modello occidentale[40].

Al contempo, l'India, il Paese più popoloso del mondo[41], sta emergendo come un importante polo per l'intelligenza artificiale, assumendo un ruolo sempre più rilevante nella definizione delle politiche digitali e delle strategie legate alle infrastrutture, con l'ambizione di trasformarsi in una potenza tecnologica globale entro il 2047. Nel 2024, il governo indiano ha promosso il piano *India AI Mission*, con lo scopo di creare un ecosistema dell'intelligenza artificiale nazionale completo che promuova l'innovazione responsabile e inclusiva, democratizzando l'accesso, migliorando la qualità dei dati, sviluppando capacità di intelligenza artificiale, attirando i migliori talenti, fornendo capitale di rischio per l'avvio imprenditoriale, garantendo progetti innovativi di impatto sociale e promuovendo l'IA etica[42]. Tale programma si inserisce nel più ampio framework della *Digital India Initiative*, lanciata nel 2015 dal Ministero dell'elettronica e dell'informatica con lo scopo di rafforzare tecnologicamente il Paese e la consapevolezza digitale[43], prevedendo tre

[40] I.A. FILIPOVA, *Legal Regulation of Artificial Intelligence: Experience of China*, in *Journal of Digital Technologies and Law, 2024*; A.H. ZHANG, *High Wire: How China Regulates Big Tech and Governs Its Economy*, in *Oxford University Press,* 2024.

[41] Per un approfondimento si consulti il sito: https://data.worldbank.org/indicator/SP.POP.TOTL?locations=IN.

[42] Per un approfondimento si consulti il seguente indirizzo *Internet*: https://www.india.gov.in/website-indiaai-mission.

[43] Ministry of Electronics and Information Technology, *Digital India Programme*, 2015.

principali pilastri: la creazione di infrastrutture digitali come servizio pubblico, la fornitura di servizi governativi *on-demand* e l'alfabetizzazione digitale dei cittadini.

Il governo locale e il settore privato stanno, quindi, investendo molto in infrastrutture, data center e formazione. L'esigenza di garantire la sovranità digitale nazionale ha acquisito urgenza poiché le dipendenze globali dalle tecnologie di IA rappresentano rischi per la sicurezza nazionale, la *privacy* e l'indipendenza economica[44]. Va, altresì, considerato che il quadro complessivo della sicurezza informatica continua a presentare rilevanti criticità, i meccanismi istituzionali appaiono frammentati, si rileva un marcato divario digitale e manca un'infrastruttura solida[45]. Attualmente, la *governance* indiana dei dati si fonda sul *Digital Personal Data Protection Act*, entrato in vigore l'11 agosto 2023. Esso rappresenta il culmine di un lungo processo di riforma iniziato con la sentenza della Corte Suprema indiana nel caso Justice K.S Puttaswamy v. Union od India del 2017, che ha riconosciuto il diritto alla *privacy* come diritto fondamentale ai sensi dell'art. 21 della Costituzione indiana[46].

In tale scenario, occorre evidenziare che l'implementazione di sistemi basati sull'uso dell'intelligenza artificiale – nel Paese – non rappresenta solo uno strumento per l'innovazione, ma un abilitatore strategico per risolvere le più urgenti criticità socio-economiche, tra cui, ad esempio, il potenziamento delle prestazioni e dell'assistenza sanitaria, il miglioramento delle rese agricole, l'aumento della produttività industriale, la crescita nelle aree sotto servite. Nonostante sia ancora assente una normativa specifica sull'intelligenza artificiale, i tentativi di regolamentare il settore digitale in India non sono nuovi e si articolano in interventi settoriali, *policy papers* e linee guida[47].

---

[44] P. PANDEY, *Digital Sovereignty and AI: Developing India's National AI Stack for Strategic Autonomy*, in *Procedia Computer Science*, 2025, pp. 250-259.

[45] A. CHAKRABORTY, S. TIWARI, *An analytical study on challenges and gaps in India's cyber security framework*, in *Int. J. Criminal Common Statutory Law*, 2025. Per un approfondimento, si va: S. SURENDRAN, R. SIBY, *A deep dive into cybercrime legal framework of India*, in *SSRN*, 2025.

[46] Per un approfondimento sul tema si veda V. BHANDARI, A. KAK, S. PARSHEERA & F. RAHMAN, *An Analysis of Puttaswamy: The Supreme Court's Privacy Verdict*, in *IndraStra Global*, 2017.

[47] Tra gli altri, rilevano: Information Technology Act del 2000; National Strategy for Artificial Intelligence del 2018; Principi per un'IA responsabile del 2021, Digital Personal Data Protection Act del 2023, Competency Framework for AI Integration in India del 2025.

Il caso indiano risulta particolarmente significativo poiché mette in luce le molteplici sfaccettature del concetto di sovranità digitale, offrendo una triplice chiave interpretativa. In primo luogo, la "retorica anticoloniale", che richiama e denuncia, come nel caso africano, l'estrazione dei dati da parte degli attori stranieri, configurando la sovranità digitale come strumento di autodeterminazione; in secondo luogo, la "retorica tecnologica-nazionalista" che collega lo sviluppo tecnologico alla sicurezza nazionale, finanziando la costruzione di infrastrutture critiche sul territorio e la delocalizzazione delle industrie digitali strategiche; infine, la "retorica liberale-democratica" che enfatizza la protezione dello stato di diritto e il modello democratico[48]. Tali interpretazioni si traducono in concreti strumenti di potere, ad esempio: il governo ha spesso utilizzato la sovranità digitale per giustificare controlli più stringenti sulle piattaforme digitali, incluse le richieste di tracciabilità dei messaggi e rimozione di contenuti, nonché divieti per applicazioni, come nel caso di *Tik Tok* nel 2019 e nel 2020[49], evidenziando l'intersezione tra sicurezza nazionale, interessi economici e tensioni geopolitiche.

Il progetto di legge sull'intelligenza artificiale (*Digital India Bill*) e le proposte di regolamentazione settoriale dell'IA elaborate dalla *National Institution for Trasforming India* evidenziano un approccio che privilegia l'autoregolamentazione del mercato rispetto a vincoli normativi stringenti. Da un lato, infatti, si evita un'eccessiva rigidità normativa che potrebbe rallentare l'implementazione e l'adozione di sistemi tecnologici innovativi, privilegiando una maggiore flessibilità; d'altro canto, si esclude una strategia puramente orientata al mercato, privilegiando e investendo in una efficace collaborazione tra il settore pubblico e quello

[48] K. DATTANI, *Spectrally shape-shifting: biometrics, fintech and corporate-state in India*, in *Journal of Cultural Economy*, 2023; S. GUPTA, R. SONY, *Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace*, in *Legal Issues in the Digital Age*, 2021.

[49] Ai sensi dell'Information Technology Act, nel 2020, il Governo dell'India ha bloccato più di cinquanta applicazioni, disponibili sulle piattaforme Android e iOS, denunciate di pregiudicare la sovranità e l'integrità dell'India, la sicurezza dello Stato e l'ordine pubblico, attraverso il furto e la trasmissione non autorizzata dei dati degli utenti a server situati al di fuori del Paese. L'India ha bloccato l'utilizzo di Tik Tok due volte, nell'aprile 2019 a seguito di una causa legale con i danni che causava ai giovani indiani, e nel giugno 2020 a seguito degli scontri di confine tra India e Cina, in cui morirono diversi soldati indiani e cinesi. Per un approfondimento si vedano: A. KUMAR, D. THUSSU, *Media, digital sovereignty and geopolitics: the case of Tik Tok ban in India,* in *Sage Journal*, 2023; M. JIANG, *Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa*, in *P&I*, 2024.

privato. Tuttavia, vige una molteplicità di autorità che rischia di generare sovrapposizioni e difficoltà di coordinamento; infatti, la competenza è ripartita tra diversi organismi: il *Data Protection Board of India*, istituito dal DPDP *Act* del 2023; la *Telecom Regulatory Authority of India*; il *Computer Emergency Response Team*, operante entro i limiti descritti dall'*Information Technology Act*; oltre ad altre autorità settoriali, come la *Reserve Bank of India*. Inoltre, ai sensi di quanto previsto dal settimo allegato della Costituzione, anche gli Stati godono di competenze concorrenti nelle materie digitali.

L'approccio indiano si fonda, quindi, su un delicato bilanciamento tra innovazione e responsabilità, con lo scopo di orientarsi a un modello ibrido tra l'approccio europeo, cinese e quello statunitense. A differenza del modello statunitense, che si distingue per un approccio più frammentato e settoriale, l'India presenta un sistema più uniforme. Analogamente al *GDPR* e all'*AI Act*, il sistema indiano adotta un approccio basato sul rischio, prevedendo garanzie rafforzate per i sistemi più critici; tuttavia, a differenza del modello europeo fondato su un'autorità indipendente di controllo[50], il *Data Protection Board* indiano è soggetto a una maggiore influenza governativa sia nella composizione che nel funzionamento[51]. Quanto al modello cinese, caratterizzato da una forte integrazione tra sicurezza nazionale e *governance* dei dati – si pensi alla *Personal Information Protection Law* del 2021 e alla *Data Security Law* del 2021 – l'India valorizza la sovranità digitale, ma assicura, almeno sul piano formale, un margine più ampio al controllo giurisdizionale indipendente.

Il modello indiano, dunque, oscilla tra le aspirazioni democratiche e le pratiche autoritarie, tra l'esigenza di aprirsi al mercato globale e la volontà di mantenere una forte sovranità digitale, tra l'impegno rivolto all'inclusione e le, ancora, marcate disuguaglianze nell'accesso alle tecnologie[52]. In questo contesto, comprendere le esigenze sociali, le aspirazioni e le preoccupazioni etiche diventa essenziale per delineare l'approccio, del Paese, all'intelligenza artificiale e, in generale, alla transizione tecnologica.

Infine, in Africa, il tema della sovranità digitale assume particolare rilievo poiché il continente ha dimostrato un forte interesse nelle strategie

[50] Artt. 51-59, GDPR.
[51] Artt. 18-19, DPDPA.
[52] N. TEWATHIA, A. KAMATH, P.VIGNESWARA ILAVARASAN, Social *inequalities, fundamental inequities, and recurring of the digital divide: Insights from India*, in *Technology in Society*, 2020.

legate allo sviluppo dell'intelligenza artificiale e delle nuove tecnologie per affrontare rilevanti sfide in diversi settori ma si scontra con una realtà ricca di profonde criticità strutturali, carenze infrastrutturali, risorse e competenze limitate, scarsità di dati e condizioni socio-economiche eterogenee. A complicare ulteriormente la situazione vi è la mancanza di una struttura politica efficiente, di politiche omogenee e di un quadro normativo uniforme[53]. Proprio in considerazione del contesto socio, economico, politico nel quale versa il continente africano, le preoccupazioni circa l'impatto dell'intelligenza artificiale sui mercati del lavoro, sulle dinamiche sociali e sulle considerazioni etiche sono al centro del dibattito. L'automazione delle attività quotidiane e l'implementazione di nuovi sistemi minacciano di sconvolgere i modelli occupazionali tradizionali in un territorio che risulta fortemente svantaggiato; inoltre, i dilemmi etici relativi alla *privacy*, all'uso dei dati e ai pregiudizi algoritmici, che colpiscono tali popolazioni, sottolineano la necessità di efficaci strategie ed efficienti politiche digitali[54].

Tuttavia, i Paesi africani sono consapevoli del potenziale di tali tecnologie e stanno orientando il loro impegno nel potenziamento della strategia digitale[55]. La frammentazione normativa caratterizza il panorama africano: mentre alcuni Stati hanno adottato legislazioni organiche, ad esempio, sulla protezione dei dati, altri presentano ancora lacune legislative significative[56]. Permangono, altresì, significative disparità in tutto il continente circa lo sviluppo di ecosistemi favorevoli all'innovazione tecnologica: secondo il *Government AI Readiness Index 2024*[57], Mauritius, Egitto e Kenya si posizionano all'apice della classifica,

---

53 D. OKAIBEDI EKE, K. WAKUNUMA, S. AKINTOYE, G. OGOH, *Trustworthy AI, African Perspectives*, Londra, 2025.

54 A. ADE-IBIJOLA, C. OKONKWO, *Artificial intelligence in Africa: emerging challenges*, in D.O. EKE, K. WAKUNUMA, S. AKINTOYE (a cura di), R*esponsible AI in Africa. Social and Cultural Studies of robots and AI*, Palgrave Macmillan, 2023; N. PASIPAMIRE, A. MUROYIWA, *Navigating algorithm bias in AI: ensuring fairness and trust in Africa*, in *Front. Res. Metr. Anal*., 2024.

55 F. AZAROUAL, *Artificial Intelligence in Africa: Challenges and Opportunities*, Policy Center for the New South, 2024.

56 A titolo esemplificativo, il Protection of Personal Information Act – POPIA – emanato nel 2013 ed entrato in vigore nel 2021 in Sud Africa; il Nigeria Data Protection Regulation aggiornato nel 2023, in Nigeria. Per un approfondimento, si vedano A. ROOS, *The European Union's General Data Protection Regulation and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'*, in *Comparative and International Law Journal of Southern Africa*, 2020; S. VICTOR, *Data Protection and Compliance in Nigeria: Challenges and Opportunities*, 2025.

57 Oxford Insights, *Government AI Readiness Index,* 2024.

evidenziando il loro impegno e i progressi compiuti nell'adozione delle politiche digitali. L'Unione Africana ha riconosciuto la necessità di un approccio coordinato attraverso l'adozione della *Digital Transformation Strategy for Africa* (2020-2030) che mira a creare un mercato digitale unico africano.

Sul piano normativo sovranazionale, la Convenzione dell'Unione Africana sulla cybersicurezza e la protezione dei dati personali – Convenzione di Malabo, 2014 – costituisce il primo strumento vincolante a livello continentale, che stabilisce i principi fondamentali per il trattamento dei dati, in linea con gli standard internazionali.

Nel 2018 è stato pubblicato il *Piano Strategico Digital Mauritius 2030* che ha posto le basi per affrontare la transizione digitale del Paese, definendo una *governance* più efficace e reattiva alle esigenze dei cittadini, ed è entrato in vigore il *Data Protection Act* del 2018, un quadro normativo completo, applicabile a livello locale, che disciplina l'accesso e l'utilizzo dei dati personali da parte di individui ed enti pubblici. Tale quadro normativo si distingue per completezza, prevedendo, altresì, la figura del *Data Protection Officer*. La *Data Protection Commission* mauriziana ha, inoltre, adottato, nel 2020, specifiche linee guida per l'uso dell'intelligenza artificiale nel settore pubblico, richiedendo valutazioni d'impatto obbligatorie per ogni sistema decisionale automatizzato che incida sui diritti fondamentali.

L'Egitto si è mostrato tempestivo nel creare, nel 2019, il Consiglio nazionale egiziano per l'IA, incaricato di esaminare le implicazioni di tale tecnologia e nel pubblicare la propria Strategia nazionale. Anche il governo keniota si è impegnato istituendo, nel 2018, una *task force* dedicata all'IA con l'obiettivo di formulare una strategia nazionale in materia e posizionare il Kenya come *hub* globale per promuovere l'adozione delle tecnologie in molteplici settori. Tale iniziativa ha prodotto, nel 2022, il *Kenya National Artificial Intelligence Strategy*, che prevede l'istituzione di un *AI Ethics Board* e l'adozione di principi etici vincolanti per lo sviluppo di sistemi di IA nel settore pubblico, con particolare riferimento ai sistemi di identificazione biometrica[58].

[58] J. AKELLO, Artificial intelligence in Kenya. Policy brief, in Paradigm Initiative, 2022; K. DIALLO, J. SMITH, C.T. OKOLO, D. NYAMWAYA, J. KGOMO, R. NGAMITA, *Case Studies of AI Policy Development in Africa*, in *Data & Policy, Cambridge University Press*, 2024. Si veda anche: J.O. CHIMAKONAM, *Algorithmic Colonization of Africa*, in S. CAVE, K. DIHAL, S. DILLON (eds.), *Imaginig AI: How the World Sees Intelligent Machines*, in *Oxford University Press*, 2023.

Nel luglio 2024 l'Unione Africana ha mostrato un importante segnale adottando la Strategia Continentale per l'Intelligenza Artificiale, che costituisce il primo *framework* organico per la *governance* dell'IA a livello continentale. Tale iniziativa ambisce a orientare lo sviluppo delle nuove tecnologie secondo principi etici, responsabili ed equi, in linea con l'Agenda 2063 per la trasformazione economica e sociale dell'Africa ed enfatizza la necessità per gli Stati membri di costruire competenze adeguate, di favorire l'uguaglianza e orientare la crescita verso nuove opportunità emergenti di sviluppo in settori come l'agribusiness, le infrastrutture, la salute, l'istruzione e le materie prime di cui l'Africa è ricca.

Le evidenze empiriche confermano l'impatto positivo delle applicazioni di intelligenza artificiale già operative nel continente, che forniscono soluzioni alle principali sfide sociali, economiche, ambientali; si pensi, a titolo esemplificativo, al settore sanitario, all'istruzione, all'agricoltura[59]. Tale distribuzione settoriale riflette, chiaramente, le priorità di sviluppo e il riconoscimento del potenziale dell'IA nell'affrontare le sfide più urgenti.

Risulta, tuttavia, fondamentale evidenziare come l'avanzamento tecnologico, da solo, non sia sufficiente. Le criticità evidenziate, dalla dipendenza straniera al colonialismo algoritmico, dai *bias* al deficit infrastrutturale, rappresentano degli ostacoli significativi che rischiano di amplificare le dinamiche di subordinazione e marginalizzazione.

Centrale, infatti, risulta il dibattito sul monopolio sui dati africani da parte delle società tecnologiche straniere, soprattutto statunitensi e cinesi, le quali, in assenza di regolamentazioni robuste esercitano pratiche di *data mining* intensive, non permesse nelle proprie giurisdizioni. Il colonialismo dei dati rappresenta una nuova forma di appropriazione che trasferisce i processi coloniali storici in una nuova dimensione digitale, caratterizzata

[59] Per un approfondimento, si vedano alcuni esempi di iniziative: *Masakhane*: iniziativa panafricana per integrare completamente le lingue africane nelle tecnologie; *AI Hub*: piattaforma per la ricerca e la formazione sull'IA applicata con lo scopo di sviluppare soluzioni pratiche per settori come la salute, l'agricoltura e la finanza; *Awa*: sistema di intelligenza artificiale di lingua Wolof per fornire ai senegalesi l'accesso diretto ai servizi digitali (tra cui, l'accesso all'assistenza sanitaria) nella loro lingua madre; *IRCAD Africa* e *DOCTORAI*: per la formazione medica e le diagnosi mediche in Ruanda; *UMMISCO Research Unit*: per la lotta contro le epidemie alle piante. Per un ulteriore approfondimento si consulti: https://www.afd.fr/en/Artificial-intelligence-Africa.

dallo sfruttamento degli esseri umani, appartenenti ai contesti più svantaggiati, attraverso i dati[60].

Pertanto, la sfida fondamentale per l'Africa è quella di costruire una sovranità digitale autentica, in cui la dimensione giuridica e un solido impianto istituzionale risultano cruciali per l'autonomia politica ed economica.

5. Considerazioni conclusive

Il panorama delineato evidenzia come ciascuna Nazione stia cercando di definire politiche su misura, capaci di rispondere alle specifiche esigenze locali, perseguendo un percorso di innovazione etico, responsabile e sostenibile. Tali strategie non si limitano alla semplice implementazione tecnologica, ma riflettono la crescente consapevolezza dell'importanza della sovranità digitale, intesa come capacità di controllo e tutela delle risorse, dei dati e delle infrastrutture.

Alla luce dell'analisi condotta, per conseguire un elevato livello di efficienza, risultano essenziali: un solido piano di investimento nella ricerca e nello sviluppo, con lo scopo di rafforzare la propria competitività tecnologica; la promozione della formazione e dell'alfabetizzazione digitale, per garantire che cittadini, imprese e istituzioni siano pienamente consapevoli e preparati per beneficiare delle opportunità e riconoscere i rischi; lo sviluppo di un quadro normativo solido, in grado di regolamentare in maniera coerente lo sviluppo delle nuove tecnologie, senza ostacolare l'innovazione; e, infine, la cooperazione internazionale, fattore essenziale per coordinare le strategie digitali nazionali e consolidare le alleanze tecnologiche a livello globale.

---

[60] Per un approfondimento sul tema, si vedano A.O. SALAMI, *Artificial Intelligence, digital colonialism and the implications for Africa's future development*, in *Cambridge University Press*, 2024; N. COULDRY, U.A. MEJIAS, *Data Colonialism: Rethinking Big Data's Relation to the Comtemporary Subject*, in *Television & New Media*, 2019, pp. 336-349; A.B. MAKULILO, *African Data Privacy Laws*, Springer, 2016; L. FLORIDI, *The Fight for Digital Sovereignty: What It is, and Why It Matters*, in *Philosophy & Technology*, 2020, pp. 369-378.

L'*AI Act* e il *risk-based approach* nel settore digitale dell'UE al crocevia tra elementi di continuità e innovazione

di MARIO CARTA* e MARCO GUIDI**

SOMMARIO: 1. Introduzione. – 2. Il ruolo del *risk-based approach* per l'*AI Act*. – 2.1. L'anticipazione e la graduazione del rischio ai sensi dell'*AI Act*. – 2.1.1. L'approccio basato sul rischio dell'*AI Act* e la normativa sulla sicurezza dei prodotti: profili di continuità… – 2.1.2. …e di discontinuità – 3. L'approccio basato sul rischio dell'*AI Act* e la disciplina sulla protezione dei dati personali: profili di continuità e discontinuità. – 3.1. L'approccio basato sul rischio nella disciplina sulla protezione dei dati personali. – 3.2. L'approccio basato sul rischio: il confronto tra GDPR e *AI Act*. – 3.2.1. Il primo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: l'imposizione dei divieti. – 3.2.2. Il secondo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: la tutela rafforzata dei soggetti vulnerabili. – 3.2.3. Il terzo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: la gestione del rischio. – 4. Conclusioni.

1. Introduzione

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (cd. *AI Act*)[1] è stato oggetto, da parte degli studiosi del diritto appartenenti a

* Professore ordinario di diritto dell'Unione europea presso l'Università degli Studi di Roma UnitelmaSapienza, Direttore del Dipartimento di Diritto e Società Digitale.

** Ricercatore TDA di diritto dell'Unione europea presso l'Università degli Studi di Roma UnitelmaSapienza, Dipartimento di Diritto e Società Digitale.

Sebbene il presente contributo sia frutto di riflessioni comuni e condivise, Mario Carta è autore dei §§ 1, 2, 2.1 e 2.1.1, Marco Guidi è autore dei §§ 2.1.2, 3, 3.1, 3.2, 3.2.1, 3.2.2, 3.2.3. Il § 4 è, invece, da imputarsi ad entrambi gli autori.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) 300/2008, (UE) 167/2013, (UE) 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in *GUUE* L 2024/1689 del 12 luglio 2024. Per una prima introduzione sul tema v. F. FERRI (a cura di), *L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive*, in *Rivista Quaderni AISDUE - fascicolo speciale 2/2024*, p. 1; A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *La rivoluzione dell'intelligenza artificiale: profili giuridici*, Bologna, 2022; G.M. RICCIO, G. ZICCARDI, G. SCORZA (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, 2022; C. CAMARDI, *La via europea per l'intelligenza artificiale*, Padova, 2022, p. 1; G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021; G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 1; S. DORIGO, *Il ragionamento giuridico nell'era dell'intelligenza*

diversi settori, di un ampio e approfondito dibattito, avviatosi già prima che si concludesse il suo tortuoso processo di adozione, il 12 luglio 2024, con la pubblicazione nella Gazzetta Ufficiale dell'UE[2].

L'interesse suscitato dall'*AI Act* oltre ad essere ascrivibile alla tempistica della sua approvazione – trattandosi di una tra le prime normative adottate, a livello globale, in questo settore[3] – è legato in

artificiale, Pisa, 2020, p. 1; U. RUFFOLO, *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020, p. 1. Per un inquadramento economico v. W. SIMONS, A. TURRINI, L. VIVIAN, *Artificial Intelligence: Economic Impact, Opportunities, Challenges, Implications for Policy*, Discussion Paper No. 210, 2024. Sia consentito infine il rinvio a M. CARTA*, Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, in *Eurojus,* 2024, pp. 188-204.

[2] Il processo di adozione dell'*AI Act* ha avuto avvio con la Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e che modifica alcuni atti legislativi dell'Unione, presentata dalla Commissione il 21 aprile 2021, COM(2021) 206 def. A questa hanno fatto seguito l'orientamento generale del Consiglio dell'Unione europea adottato il 6 dicembre 2022 (Doc. ST-14954-2022-INIT) e la posizione negoziale del Parlamento europeo approvata il 14 giugno 2023 (TA-9-2023-0236). Infine, nel dicembre 2023, Parlamento e Consiglio hanno raggiunto un accordo politico in trilogo sul testo, poi approvato dal Parlamento europeo il 13 marzo 2024 (P9_TA(2024)0138) e adottato dal Consiglio il 21 maggio 2024 (2021/0106(COD), e il testo ufficiale del regolamento è stato pubblicato nella Gazzetta Ufficiale il 12 luglio 2024. Prima della proposta di regolamento da parte della Commissione, l'iniziativa dell'UE nell'ambito dell'intelligenza artificiale si era sviluppata attraverso numerosi atti e documenti strategici, tra cui: *(i)* Comunicazione della Commissione, *L'intelligenza artificiale per l'Europa*, (COM(2018) 237 def.); *(ii)* Comunicazione della Commissione, *Creare fiducia nell'intelligenza artificiale antropocentrica*, (COM(2019) 168 def.); *(iii)* Ethics Guidelines for Trustworthy AI (High-Level Expert Group on AI, 8 aprile 2019); *(iv)* Policy and Investment Recommendations for Trustworthy AI (High-Level Expert Group on AI, 26 giugno 2019); *(v)* Libro bianco sull'intelligenza artificiale – *Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65 def.); *(vi)* Comunicazione della Commissione, *Promuovere un approccio europeo all'intelligenza artificiale*, (COM(2021) 205 def.); (vii) Piano coordinato sull'intelligenza artificiale, avviato nel 2018 (COM(2018) 795 final) e aggiornato nel 2021 (COM(2021) 205 def.).

[3] Sebbene la proposta della Commissione europea del 21 aprile 2021 sia stata la prima iniziativa legislativa organica a livello globale in materia di intelligenza artificiale, l'approvazione definitiva dell'*AI Act* è intervenuta successivamente rispetto all'adozione del "*Act concerning consumer protections in interactions with artificial intelligence systems-Senate Bill 24-205*" ("Colorado Artificial Intelligence Act" o "CAIA"), promulgato il 17 maggio 2024, che rappresenta il primo quadro normativo statunitense di regolazione generale dei sistemi di IA. Sul versante statunitense, a livello federale, si segnalano inoltre il "*Blueprint for an AI Bill of Rights - making automated systems work for the American people*", adottato dalla *White House Office of Science and Technology Policy* nell'ottobre 2022 e lo "*Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*", firmato dal Presidente Biden il 30 ottobre 2023 e revocato dal successivo "*Removing barriers to American leadership in artificial intelligence*, firmato dal Presidente Trump il 23 gennaio 2025. Al di fuori del contesto occidentale, occorre segnalare l'iniziativa della Repubblica Popolare

maniera significativa sia al suo esteso ambito di applicazione sia alla complessità e innovatività dell'impianto regolatorio che lo caratterizza.

Sotto il primo profilo, infatti, il regolamento si configura quale disciplina di carattere orizzontale, applicabile a tutti i cd. sistemi e modelli di IA, indipendentemente dal settore d'impiego, ad eccezione di quelli militare, di difesa e di sicurezza nazionale, espressamente esclusi dall'art. 2, par. 3, in ossequio all'art. 4, par. 2, TUE[4].

Sotto il secondo profilo, le numerose novità introdotte dall'*AI Act* hanno dato origine ad una cospicua e ricca attività di interpretazione da parte della dottrina. Tra le principali possono citarsi, senza pretesa di esaustività: (*i*) la previsione, all'art. 3, di un articolato impianto definitorio che non si limita ai concetti di "sistema di IA"[5] e di "modello di IA"

Cinese con le cd. *Provisional Measures for the Management of Generative Artificial Intelligence Services*, adottate dalla *Cyberspace Administration of China* il 10 luglio 2023 ed entrate in vigore il 15 agosto 2023, che costituiscono il primo intervento regolatorio specificamente dedicato ai sistemi di IA generativa. Per un approfondimento v. A. LALLI, *I non radicalmente diversi approcci alla regolazione dell'intelligenza artificiale in Europa, Stati Uniti e Cina*, in A. LALLI (a cura di), *La regolazione pubblica delle tecnologie digitali e dell'intelligenza artificiale*, Torino, 2024, p. 115; M. KARANICOLAS, *Artificial Intelligence and Regulatory Enforcement - report to the Admin. Conf. of the U.S.*, 9 dicembre 2024; A.H. ZHANG, *The Promise and Perils of China's Regulation of Artificial Intelligence*, in *Columbia Journal of Transnational Law*, 2024, p. 2; G. CAPUZZO, *A(I) Minority Report. Uno studio su intelligenza artificiale e comparazione giuridica tra UE, USA e Cina*, in *Rivista critica del diritto privato*, 2022, p. 479.

[4] Questa scelta, su espressa precisazione del Consiglio dell'UE (Interinstitutional File 2021/0106(COD) del 26 gennaio 2024, ricalca l'impostazione precedente del Regolamento (Ue) 2024/2847 sulla ciberresilienza (art. 2, par. 7) e del Regolamento (UE) 2023/2854 sui dati, cd. *Data Act* (art. 1, par. 6). Sull'uso di sistemi di IA in ambito militare, il Parlamento europeo si è distinto quale Istituzione dell'UE più attiva, come testimoniato dall'adozione della *Risoluzione del 12 settembre 2018 sui sistemi d'arma autonomi* (2018/2752(RSP)), della *Risoluzione del 18 gennaio 2023 sull'attuazione della politica di sicurezza e di difesa comune — relazione annuale 2022* (2022/2050(INI)), della *Risoluzione del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale* (2020/2013(INI)), nonché del *briefing* dell'11 aprile 2025, *European Parliament, Defence and artificial intelligence*. In dottrina v. A. CIVITELLA, *Riflessioni sull'impatto dell'intelligenza artificiale sul rispetto del diritto internazionale umanitario e il ruolo del principio di umanità*, in *MediaLaws - Rivista di Diritto dei Media*, 1/2025, p. 162; K. YORDANOVA, *Artificial Intelligence and Armed Conflicts*, in N.A. SMUHA (a cura di), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, Cambridge, 2025, p. 411; M. SCHMITT, J. THURNHER, *"Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, in *Harvard National Security Journal*, 2013, p. 231.

[5] Cfr. European Commission, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, C(2025) 5053

(inclusi quelli a finalità generale) [6] e ai relativi *output*, come i cd. *deepfake*[7], ma si estende a un insieme più ampio di nozioni tecniche e giuridiche. Vi sono ricompresi, da un lato, l'ampio catalogo delle tipologie di dati, nel quale figurano oltre le categorie tradizionali di dati "personale" e "non personale", quelle inedite di dati di "addestramento", "convalida", "prova", "input", e "operativi sensibili"[8]; dall'altro lato, la biometria, la cui estensione funzionale ricomprende la "identificazione" e la "verifica", attraverso sistemi "di riconoscimento delle emozioni", "di categorizzazione biometrica" e "di identificazione biometrica remota", "in tempo reale" o "a posteriori"[9]; (*ii*) l'alfabetizzazione in materia di IA che, *ex* art. 4, obbliga i fornitori e i *deployer* dei sistemi di IA ad adottare

---

final, para. 9 e 10, secondo cui i sistemi di IA constano di sette attributi principali: (1) un sistema basato su macchine; (2) progettato per funzionare con diversi livelli di autonomia; (3) che può mostrare capacità di adattamento dopo l'implementazione; (4) e che, per obiettivi espliciti o impliciti; (5) deduce, dagli input che riceve, come generare output (6) quali previsioni, contenuti, raccomandazioni o decisioni (7) che possono influenzare ambienti fisici o virtuali. Tale definizione di sistema di IA, *ex* art. 3, punto 1, *AI Act*, è coerente con quella stabilita sul piano internazionale, segnatamente dalla Convenzione quadro Council of Europe, *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CM(2024)52-final, nonché dal *Explanatory memorandum on the updated OECD definition of an AI system*, OECD artificial intelligence papers, n. 3, 2024, disponibile online all'indirizzo www.oecd-ilibrary.org/science-and-technology/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en. In dottrina, v. G. BARONE, *Giustizia predittiva e certezza del diritto*, Pisa, 2024, p. 9; P. WANG, *On Defining Artificial Intelligence*, in *Journal of Artificial General Intelligence*, 2019, p. 1.

[6] Relativamente ai "modelli di IA", il regolamento non ne fornisce una definizione nell'articolato normativo. Il considerando 7, tuttavia, specifica che «[s]ebbene i modelli di IA siano componenti essenziali dei sistemi di IA, essi non costituiscono di per sé sistemi di IA. I modelli di IA necessitano dell'aggiunta di altri componenti, ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte. Il presente regolamento stabilisce norme specifiche per i modelli di IA per finalità generali». La definizione di modello di IA a finalità generale è prevista dall'art. 3, punto 63, *AI Act* quale modello di IA «caratterizzato una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti […] e che può essere integrato in una varietà di sistemi o applicazioni a valle». Si rinvia a OECD, *G7 Hiroshima Process on Generative Artificial Intelligence (AI): Towards a G7 Common Understanding on Generative AI*, Parigi, 2023; C. NOVELLI ET AL., *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, in *Computer Law & Security Review*, 2024, p. 1; European Commission, *Living Guidelines on the Responsible Use of Generative AI in Research*, ERA Forum Stakeholders' document, 2024;

[7] Ai sensi dell'art. 3, punto 60, per "deep fake" si intende: «un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona».

[8] Cfr. art. 3, rispettivamente punti 50, 51, 29, 30, 32, 33 e 38.

[9] Cfr. art. 3, rispettivamente punti 35, 36, 39, 40, 41, 42 e 43.

«misure per garantire […] un livello sufficiente di alfabetizzazione in materia di IA del loro personale», sulla base delle «conoscenze tecniche», del «contesto in cui i sistemi di IA devono essere utilizzati» e, infine, degli utenti che presumibilmente faranno uso di tale sistema di IA; (*iii*) l'affermazione del principio della sorveglianza umana di cui all'art. 14, che impone di garantire, lungo l'intero ciclo di vita dei sistemi di IA, l'esistenza di efficaci strumenti di supervisione da parte di persone fisiche[10], in coerenza con l'approccio antropocentrico dell'*AI Act*, secondo cui l'intelligenza artificiale deve rimanere uno strumento al servizio dell'uomo[11]; (*iv*) lo spazio di sperimentazione normativa per l'IA (cd. *regulatory sandbox*) il quale, *ex* art. 57, si configura quale «ambiente controllato di sperimentazione e prova nella fase di sviluppo e pre-commercializzazione al fine di garantire la conformità dei sistemi di IA innovativi» ai requisiti imposti dal regolamento. In virtù della sua natura, tale spazio è escluso dall'ambito di applicazione materiale del regolamento, allo scopo di «sostenere l'innovazione» e «rispettare la

[10] D. MARTIRE, Human in the loop*. L'essere umano come fattore condizionante della – o condizionato dalla – intelligenza artificiale*, in *Rivista italiana di informatica e diritto*, 2024, p. 467; M. PAOLANTI, *IA e moderazione dei contenuti sui social media: il principio del "*Human in the loop*" nel campo del diritto all'informazione e alla comunicazione*, in *MediaLaws – Rivista del diritto dei media*, 1/2024, p. 85. La "sorveglianza umana" costituisce un principio innovativo, pur trovando un antecedente concettuale nell'art. 22 GDPR. Tuttavia, come si avrà modo di osservare nel prosieguo, nell'ambito dell'art. 22 GDPR l'intervento umano è previsto quale mera clausola di salvaguardia nel contesto delle decisioni automatizzate fondate sul trattamento di dati personali, mentre l'*AI Act* eleva tale principio a requisito strutturale, imponendo la progettazione di sistemi di IA che consentano un'effettiva supervisione umana lungo tutte le fasi della loro programmazione, test e utilizzo.

[11] Comunicazione della Commissione europea, *Creare fiducia nell'intelligenza artificiale antropocentrica*, cit., p. 1 secondo cui: «[l]a strategia europea per l'IA e il piano coordinato sull'IA indicano chiaramente che la fiducia è una condizione indispensabile per assicurare un approccio antropocentrico all'IA: l'intelligenza artificiale non è fine a se stessa, ma è uno strumento a servizio delle persone che ha come fine ultimo quello di migliorare il benessere degli esseri umani. Per questo occorre garantire l'affidabilità dell'IA. I valori su cui si basano le nostre società devono essere pienamente integrati nelle modalità di sviluppo dell'IA.» Tale orientamento è stato fatto proprio anche dalla Dichiarazione europea sui diritti e i principi digitali per il decennio digitale 2023/C 23/01, in *GUUE* C 23 del 23 gennaio 2023, p. 1, ove si sostiene più volte che la strategia dell'UE per la trasformazione digitale «*mette al centro le persone*». (par. 6, 7 e 10). Sul concetto di IA antropocentrica v. A. PIROZZOLI, *The Human-centric Perspective in the Regulation of Artificial Intelligence*, in *European Papers*, 1/2024, p. 105. Relativamente al contesto nazionale, v. F.M. MANCIOPPI, *The anthropocentric view in the bill on AI introduced by the Italian Government*, in *MediaLaws - Rivista di Diritto dei Media*, 2/2024, p. 245.

libertà della scienza» (*consideranda* 25 e 139)[12]; (*v*) l'istituzione di una *governance* stratificata, che si articola nell'"Ufficio per l'IA", nel "consiglio europeo per l'intelligenza artificiale", nel "*forum* consultivo" e nel "Gruppo di esperti scientifici indipendenti", disciplinati rispettivamente dagli artt. 64, 66, 67 e 68; e, infine, (*vi*) la creazione, *ex* art. 71, della cd. banca dati sui sistemi di IA ad alto rischio.

Si tratta solo di alcune delle novità previste, che sono state già oggetto di numerose analisi volte a metterne in rilievo, in particolare, l'impatto sotto i profili della tutela dei diritti fondamentali[13] (riservatezza e tutela dei dati personali[14], libertà di espressione[15], tutela dei minori[16], tutela della

---

[12] E. CIRONE, *Gli spazi di sperimentazione normativa nell'Unione europea: regolamentare l'innovazione tra principi e prassi applicative, in Rivista italiana di informatica e diritto*, 1/2025, p. 258; E. PERRONE, *Regulatory Sandboxes. Spazi di sperimentazione normativa per l'intelligenza artificiale*, in *MediaLaws - Rivista di Diritto dei Media*, 1/2025, p. 237; G. RUGANI, *La promozione di strumenti di co-regolazione dell'intelligenza artificiale nell'*AI Act*, con particolare riferimento alle regulatory sandboxes*, in *Quaderni AISDUE* - Fascicolo speciale n. 2/2024, p. 1.

[13] Per una prima introduzione, v. *European Union Agency for Fundamental Rights (FRA), Getting the Future Right. Artificial Intelligence and Fundamental Rights*, Lussemburgo, 2020.

[14] P. FALLETTA, A. MARSANO, *Intelligenza artificiale e protezione dei dati personali: il rapporto tra Regolamento europeo sull'intelligenza artificiale e GDPR*, in *Rivista italiana di informatica e diritto*, 1/2024, p. 119; A. MANTELERO, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI, Information Technology and Law Series, The Hague*, 2022, p. 94; F. UFERT, *AI Regulation through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI?*, in *European Papers*, 5/2020, p. 1087 ss.; G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* - European Parliamentary Research Service, Bruxelles, 2020. Sul tema v. EDPB, Opinion 28/2024 *on certain data protection aspects related to the processing of personal data in the context of AI models*, 17 dicembre 2024, nonché le decisioni del Garante per la protezione dei dati personali n. 112 del 30 marzo 2023, doc. web n. 9870832 e n. 114, 11 aprile 2023, doc. web n. 9874702, nei confronti di OpenAI, e n. 33 del 30 gennaio 2025, doc. web n. 10098477, nei confronti di DeepSeek.

[15] L. CATANZANO, *Libertà di espressione e verità artificiali. Quale marketplace of ideas nella società dell'algoritmo?,* in *MediaLaws - Rivista di Diritto dei Media*, 1/2024, p. 61; E. LLANSO' ET AL., *Artificial intelligence, content moderation and freedom of expression, Working Paper – Transatlantic Working Group on content moderation online and freedom of expression*, 2019; Council of Europe, Committee of Experts - *Draft Guidance on the implications of generative artificial intelligence for freedom of expression*, MSI-AI(2025)10, 3 giugno 2025.

[16] M.L. BORGESE, *La duplice radice dell'Intelligenza Artificiale: fra le esigenze di innovazione e la tutela dei più fragili,* in *MediaLaws - Rivista di Diritto dei Media*, 1/2024, p. 385; UNICEF, Policy Guidance on AI for Children, New York, 2021.

salute[17]), della *rule of law*[18], dell'impiego da parte delle pubbliche amministrazioni[19] – compresa l'amministrazione della giustizia[20] e del

[17] V. SALVATORE, *Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea*, Torino, 2023. L'EMA ha recentemente pubblicato un approfondimento sul tema dell'uso dell'IA nell'ambito del ciclo di vita dei prodotti medicinali, dalla loro scoperta fino alla cd. farmacovigilanza, v. European Medicine Agency, Reflection paper on the use of Artificial Intelligence (AI) in the medicinal product lifecycle, EMA/CHMP/CVMP/83833/2023.

[18] Council of Europe, *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, cit.; C. SCHEPISI, *Diritti fondamentali, principi democratici, e* rule of law*: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in *Studi sull'integrazione europea*, 2022, p. 41; S. GREENSTEIN, *Preserving the rule of law in the era of artificial intelligence (AI)*, in *Artificial Intelligence and Law*, 2022, p. 291.

[19] J. PONCE, A. CERRILLO-I-MARTÍNEZ (a cura di), *The EU Artificial Intelligence Act and the Public Sector - Humans and AI Systems in Public Administration in the light of the European Regulation on Artificial Intelligence of 2024*, Atene, 2025; D.-U. GALETTA, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in *federalismi.it*, 2023, p. 4.

[20] C. BURELLI, *Prime brevi considerazioni sul "ddl intelligenza artificiale": incompatibilità o inopportunità?*, in *Quaderni AISDUE - Fascicolo speciale n. 2/2024*, p. 237. Sul tema la Commissione europea e il Consiglio d'Europa hanno pubblicato congiuntamente, nel febbraio 2024, una nota informativa sull'utilizzo di strumenti di intelligenza artificiale generativa nell'ambito giudiziale, mettendone in rilievo i rischi ed i limiti applicativi, v. Council of Europe – European Commission for the Efficiency of Justice (CEPEJ), *Use of Generative Artificial Intelligence (AI) by judicial professionals in a work-related context. Information note prepared by the CEPEJ Working group on Cyberjustice and Artificial Intelligence* (CEPEJ-GT-CYBERJUST(2023)5final), 2024.

fisco[21] – del diritto della concorrenza[22], del diritto d'autore[23], della gestione dei flussi migratori[24], ecc.

Il presente lavoro intende mettere in luce se, e in qual modo, l'*AI Act* possa rappresentare un modello regolatorio paradigmatico per l'intero settore digitale a livello europeo, in particolare per quanto riguarda l'approccio basato sul rischio (cd. *risk-based approach*), contribuendo così all'affermazione della sovranità tecnologica dell'Unione.

2. Il ruolo del *risk-based approach* per l'*AI Act*

2.1. L'anticipazione e la graduazione del rischio ai sensi dell'*AI Act*

Come stabilito dall'art. 1 e specificato dai *considerandi* 1 e 2, l'*AI Act* prevede un quadro normativo uniforme per la progettazione, lo sviluppo, l'immissione sul mercato, la messa a disposizione e in servizio, nonché

---

[21] OECD, *Governing with Artificial Intelligence: The State of Play and Way Forward in Core Government Functions*, Parigi, 2025; L.M. PICA, *Artificial Intelligence, Tax Law and (Intelligent?) Tax Administration*, in *European Review of Digital Administration & Law*, 3/2022, p. 141.

[22] A. ABBOTT, T. SCHREPEL (a cura di), *Artificial Intelligence and Competition Policy*, Parigi, 2024; M. ALMADA, J. MARANHÃO, G. SARTOR, *Competition in and through Artificial Intelligence*, in P.L. PARCU, M.A. ROSSI, M. BOTTA (a cura di), *Research Handbook on Competition and* Technology, Cheltenham, 2024; A. PRETA, *L'economia dei dati e l'intelligenza artificiale tra politica economica, concorrenza e regolazione dei mercati*, in V. FALCE (a cura di) *Fairness e innovazione nel mercato unico digitale*, Torino, 2020, p. 173 ss.; A. PEZZOLI, A. TONAZZI, *Discriminazione e collusione tacita tra lessico, intelligenza artificiale e algoritmi*, in *Analisi Giuridica dell'Economia*, 1/2019, p. 201; A. EZRACHI, M. E. STUCKE, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Cambridge, 2016. La Commissione europea, nel gennaio 2024, ha pubblicato due inviti a presentare contributi sulla concorrenza rispettivamente nei mondi virtuali e sull'intelligenza artificiale, richiedendo informazioni ai principali operatori digitali. Tali iniziative sono state refuse nel "*Competition Policy Brief - Competition in Generative AI and Virtual Worlds*", del settembre 2024. Nell'ambito internazionale, segnatamente, il summit tenutosi a Roma il 4 ottobre 2024, le Autorità della concorrenza dei paesi membri del G7 hanno trattato delle implicazioni concorrenziali poste dai sistemi di IA, v. *G7 Competition Authorities and Policymakers' Summit Digital Competition Communiqué*.

[23] C. GRIECO, *Il diritto d'autore nell'*AI Act: Error *404* - Page Not Found?, in *Quaderni AISDUE* fascicolo speciale 2/2024, p. 1; G. ROSSI, *L'intelligenza artificiale e la definizione di "opera dell'ingegno",* in *AIDA*, 2019, p. 268; European Union Intellectual Property Office, AI and IP: The impact of artificial intelligence on intellectual property law, 2022, disponibile online all'indirizzo https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2025_Gen AI_from_copyright_perspective/2025_GenAI_from_copyright_perspective_FullR_en.pdf.

[24] M. KONTAK, *Biometric Borders Envisaged by Frontex: Fundamental Rights in the Backseat*, in *European Papers*, 2/2024, p. 621; J. BEDUSCHI, *International Migration Management in the Age of Artificial Intelligence*, in *Migration Studies*, 3/2021, p. 576.

l'uso dei sistemi di IA nell'Unione[25]. L'obiettivo è duplice: da un lato, favorire il corretto funzionamento del Mercato Unico Digitale, creando un contesto favorevole all'innovazione tecnologica e attrattivo per gli operatori economici (cd. *ecosystem of excellence*[26]); dall'altro lato, garantire «un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente» (cd. *ecosystem of trust*[27]).

La principale leva attraverso cui il regolamento persegue tali finalità è l'approccio basato sul rischio[28], la cui centralità emerge già, a livello sistematico, dalla collocazione tra le prime disposizioni della definizione

---

[25] Le definizioni di "immissione sul mercato", "messa a disposizione" e "messa in servizio" sono stabilite all'art. 3, rispettivamente ai punti 9, 10 e 11; l'uso dei sistemi di IA nell'Unione non è, invece, definito dall'*AI Act*; tuttavia, come precisato dalla Commissione europea, esso «dovrebbe essere inteso in modo ampio come comprendente l'uso o la diffusione del sistema in qualsiasi momento del suo ciclo di vita dopo essere stato immesso sul mercato o messo in servizio», cfr. European Commission, *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, 29 luglio 2025, C(2025) 5052 final., par. 14.

[26] L'espressione è impiegata dalla Commissione europea nel proprio *Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, 21 aprile 2021, COM(2021) 206 final, p. 1. Sul tema dell'IA e il mercato unico, v. M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno*?, in *Quaderni AISDUE - Fascicolo speciale n. 2/2024*, p. 9; S. DE VRIES, *Recent Trends in EU Internal Market Legislation. Bringing back the Old Concepts?*, in T. VAN DEN BRINK, V. PASSALACQUA (a cura di), *Balancing Unity and Diversity in EU Legislation*, Cheltenham, 2024, p. 17 ss.

[27] Cfr. European Commission, *Impact Assessment Accompanying the Proposal for Artificial Intelligence Act*, cit., p.1. Sul tema della IA "affidabile", v. J. LAUX, S. WACHTER, B. MITTELSTADT, *Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk*, in *Regulation & Governance*, 18/2024, p. 3; A.N. SMUHA ET AL., *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, 2021, disponibile *online* all'indirizzo *Internet*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3899991>.

[28] V. M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, in *European Journal of Risk Regulation*, 16/2025, p. 684; A. ODDENINO, *Intelligenza Artificiale e tutela dei diritti fondamentali: alcune notazioni critiche sulla recente proposta di Regolamento della UE, con particolare riferimento all'approccio basato sul rischio e al pericolo di discriminazione algoritmica,* in F. DONATI, A. PERRUCCI, A. PAJANO (a cura di), *op.cit.*, p. 165; D. LEUFER, F. HIDVEGI, A. ZORNETTA, *The Pitfalls of the European Union's Risk-Based Approach to Digital Rulemaking*, in *UCLA Law Review*, 2024, p. 156; M. WEIMER, *The Origins of "Risk" as an Idea and the Future of Risk Regulation*, in *European Journal of Risk Regulation*, 8/2017, p. 10; OECD, *Risk and Regulatory Policy: Improving the Governance of Risk*, OECD Reviews of Regulatory Reform, OECD Publishing, Parigi, 2010, p. 185.

di "rischio"[29] – inteso come «combinazione della probabilità del verificarsi di un danno e della gravità di tale danno» – all'art. 3, punto 2, quindi a seguire solo della nozione di "sistema di IA".

La scelta di adottare il *risk-based approach* trae origine da un duplice presupposto. Innanzitutto, lo sviluppo e l'utilizzo dei sistemi di IA, pur apportando significativi benefici possono comportare dei pregiudizi di tipo sia materiale che immateriale, inclusi quelli fisici, psicologici, sociali o economici (considerando 5). Tale assunto riflette gli orientamenti consolidati sul piano internazionale (norma ISO/IEC 42001:2023[30] e raccomandazione del Consiglio sull'IA dell'OECD[31]), i quali hanno messo in rilievo la natura ambivalente dell'intelligenza artificiale.

Inoltre, il regolamento riconosce espressamente la natura multiforme dei sistemi di intelligenza artificiale, qualificandoli come una «famiglia di tecnologie in rapida evoluzione» (considerando 4)[32] che, dotata di elevata versatilità, è applicabile trasversalmente a molteplici settori produttivi e ambiti sociali.

Sono tali presupposti che spiegano l'adozione, da parte dell'*AI Act*, dell'approccio basato sul rischio. Esso, infatti, si estrinseca attraverso un «insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA» la cui tipologia e contenuto sono adattati «all'intensità e alla portata dei rischi che possono essere generati» da tali sistemi (considerando 26)[33].

---

[29] Sul concetto di rischio v. V. LUPTON, *Digital Risk Society*, in A. BURGESS, A. ALEMANNO, J. ZINN (a cura di), *Routledge Handbook of Risk Studies*, Londra, 2016, p. 301; C.R. SUNSTEIN, *Beyond the precautionary principle*, in *University of Pennsylvania Law Review*, 2003, p. 1003; U. BECK, *Risk Society. Towards a New Modernity*, Londra, 1992.

[30] ISO/IEC 42001:2023, Information technology – Artificial intelligence – Management system.

[31] OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449. Mentre sul piano statunitense abbiamo il National Institute of Standards and Technology, U.S. Department of Commerce, *Artificial Intelligence Risk Management Framework* (AI RMF 1.0), 2023, disponibile online all'indirizzo https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (*NIST AI Risk Management Framework*).

[32] Commissione europea, *Impact Assessment Accompanying the Proposal for Artificial Intelligence Act*, cit., p. 2, ove si precisa che: «AI is best defined as an emerging general-purpose technology: a very powerful family of computer programming techniques that can be deployed for desirable uses.»

[33] Cfr. Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e che modifica alcuni atti legislativi dell'Unione, cit., par. 1.1, in cui la Commissione specifica che: «l'intervento legale è adattato alle situazioni concrete nelle quali sussiste un motivo di preoccupazione giustificato o nelle quali tale preoccupazione può essere ragionevolmente prevista nel prossimo futuro».

Nello specifico, tale approccio comprende due dimensioni strettamente interconnesse, ossia la valutazione del rischio, da effettuarsi a monte, e la calibrazione delle misure regolatorie, volte alla sua prevenzione e mitigazione, da svolgersi a valle.

La prima mira a stabilire un equilibrio tra la creazione di un mercato interno dell'IA e la salvaguardia degli interessi generali e pubblici, definendo quali rischi possano considerarsi accettabili e in quale misura. In questa prospettiva, il legislatore europeo ha privilegiato un controllo preventivo sull'immissione in commercio di sistemi di IA potenzialmente dannosi, piuttosto che l'accertamento a posteriori di eventuali condotte illegittime. Tale scelta riflette la consapevolezza che alcuni danni derivanti da un uso improprio o non sufficientemente controllato di tali sistemi possano risultare irreparabili o comunque non compensabili *ex post*, data la natura dei beni e dei diritti in gioco[34].

Sulla valutazione del rischio s'innesta la graduazione nella disciplina dei sistemi di IA. All'aumento del livello di rischio individuato nella fase precedente corrispondono – in ossequio al principio di proporzionalità – divieti, obblighi di conformità e adempimenti procedurali più stringenti, distribuiti tra più soggetti, a seconda del rispettivo ruolo rivestito nella catena di produzione di valore dell'IA[35].

Ne discende la classificazione dei sistemi di IA in quattro categorie di rischio, corrispondenti ad altrettanti regimi giuridici. In primo luogo, i "sistemi a rischio inaccettabile" di cui all'art. 5 sono oggetto, a far data dal 2 febbraio 2025, di un divieto di immissione sul mercato e di utilizzo, per via del loro accentuato livello di «pericolosità» e «abusività» (considerando 28). Ne fanno parte, ad esempio, i sistemi di intelligenza artificiale destinati alla manipolazione subliminale di individui o gruppi (art. 5, par. 1, lett. a), nonché quelli impiegati per la raccolta indiscriminata

[34] Cfr. C. SCHEPISI, *Diritti fondamentali, principi democratici e* rule of law*: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *op.cit.*, p. 206.

[35] Non sono stati presi, quindi, in considerazioni parametri quantitativi (fatturato, utenza attiva, consistenza base di clienti commerciali, ecc.), a differenza, invece, di altri atti adottati nel settore digitale, quali il Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in *GUUE* L 265 del 12 ottobre 2022, p. 1, cd. *Digital Market Act* e il Regolamento (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 Direttiva 2000/31/CE (regolamento sui servizi digitali), in *GUUE* L 277 del 27 ottobre 2022, p. 1, cd. *Digital Service Act*.

di dati biometrici, in particolare di immagini del volto, mediante processi automatizzati di *scraping* da fonti *online* o da registrazioni di sorveglianza, finalizzati a creare o ampliare banche dati biometriche senza il consenso o la consapevolezza delle persone interessate (art. 5, par. 1, lett. e). Il regolamento, in tale prospettiva, individua soglie di protezione inderogabili per i diritti fondamentali, come la non discriminazione, la protezione dei dati personali, la tutela della vita privata e dei minori, che non possono essere compressi da esigenze economiche o da altri diritti confliggenti (quali la libertà delle arti e delle scienze o la libertà d'impresa *ex* artt. 13 e 16 della Carta dei diritti fondamentali)[36].

In secondo luogo, l'art. 6 individua i "sistemi ad alto rischio", la cui valutazione del rischio, come precisato dalla Commissione europea nel *Libro bianco sull'intelligenza artificiale*, si fonda su due criteri cumulativi: il settore interessato e l'uso previsto[37].

Il primo criterio attiene all'individuazione degli ambiti in cui sia ragionevole prevedere rischi significativi. L'intervento normativo è così circoscritto ai contesti (merceologici o applicativi) in cui i rischi sono statisticamente più probabili e potenzialmente più gravi.

Il secondo criterio riguarda le modalità concrete di utilizzo dell'IA all'interno di tali settori "sensibili". Non ogni applicazione, infatti, genera di per sé un rischio significativo, in quanto esso varia a seconda dell'effettiva funzione svolta e dell'impatto concreto sugli individui o sulla collettività.

Il regolamento fa propria tale impostazione, distinguendo due ipotesi di sistemi di IA ad alto rischio, la cui immissione sul mercato e il cui impiego sono consentiti, a partire dal 2 agosto 2026, solo previa conformità a requisiti stringenti (Capo III, artt. 8-15).

Da un lato, rientrano in tale categoria i sistemi di IA che costituiscono componenti di sicurezza di prodotti, o che rappresentano essi stessi prodotti, disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'Allegato I e soggetti a valutazione obbligatoria di conformità prima dell'immissione sul mercato (art. 6, par. 1). Si tratta di normative settoriali relative a prodotti considerati pericolosi, quali dispositivi medici, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera

[36] European Commission, *Proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Explanatory Memorandum*, 21 aprile 2021, COM(2021) 206 def., par. 3.5.
[37] Commissione europea, *Libro bianco sull'intelligenza artificiale*, cit., pp. 19 e 20.

potenzialmente esplosiva, attrezzature a pressione, ecc. Per tali sistemi di IA, la qualifica ad alto rischio deriva automaticamente dalla natura del prodotto di riferimento.

Dall'altro lato, sono considerati ad alto rischio i sistemi di IA impiegati negli ambiti elencati nell'Allegato III (art. 6, par. 2) che sono ritenuti più rischiosi, quali istruzione e formazione, biometria, servizi essenziali, ecc.

Con riferimento a questi ultimi sistemi di IA, il legislatore ha previsto una clausola di esclusione che ne riduce il livello di rischiosità, qualora la loro effettiva destinazione d'uso non presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, come nel caso in cui il sistema di IA sia «destinato a eseguire un compito procedurale limitato» oppure sia «destinato a migliorare il risultato di un'attività umana precedentemente completata» (art. 6, par. 3).

Il regolamento individua, infine, le classi dei sistemi di IA a "rischio limitato" o a "rischio minimo", per i quali, rispettivamente, sono previsti meri obblighi di trasparenza (Capo IV, art. 50), per via della loro interazione con gli individui, e la possibilità di adesione volontaria a codici di condotta (Capo X, art. 95), con ciò rappresentando in maniera plastica la proporzionalità dell'approccio in analisi.

A queste quattro classi di sistemi di IA occorre aggiungere – per iniziativa del Parlamento europeo[38] – la disciplina dedicata ai citati modelli di IA per finalità generali, la cui natura polivalente in termini di svolgimento di compiti ulteriori e diversi rispetto a quelli originariamente previsti non ne consente una classificazione a priori basata sul rischio. Pertanto, essi sono oggetto di una disciplina *ad hoc* rispetto a quella prevista per i sistemi di IA (Capo V).

2.1.1. L'approccio basato sul rischio dell'*AI Act* e la normativa sulla sicurezza dei prodotti: profili di continuità…

L'approccio basato sul rischio e la conseguente classificazione dei sistemi di intelligenza artificiale, con graduazione proporzionale degli obblighi sostanziali e procedurali, non rappresentano una novità introdotta dall'*AI Act*, affondando, piuttosto, le proprie radici nella esperienza

[38] European Parliament, *Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, (COM(2021)0206 - C9-0146/2021 - 2021/0106(COD)).

normativa dell'Unione europea maturata in materia di sicurezza dei prodotti. Già a partire dagli anni Ottanta, in considerazione degli effetti della sentenza *Cassis de Dijon*[39], con l'adozione del cd. *New Approach* – formalizzato nella Risoluzione del Consiglio del 7 maggio 1985[40] e richiamato dal Libro Bianco "*Il completamento del mercato interno*"[41] – è stato delineato un nuovo modello di armonizzazione legislativa[42].

Tale modello prevede la definizione, da parte del legislatore dell'Unione, dei soli requisiti essenziali di sicurezza e salute, demandando invece alle norme armonizzate – elaborate dagli organismi europei di normazione (CEN, CENELEC, ETSI) su mandato della Commissione – il compito di specificare gli standard tecnici idonei a garantirne il rispetto[43]. L'adesione a tali norme, pur formalmente volontaria, conferiva al prodotto la presunzione di conformità e, conseguentemente, il diritto alla libera circolazione nel mercato interno. Tale impostazione, volta a ridurre le barriere tecniche al commercio e a rafforzare la competitività a livello "comunitario", ha segnato una tappa decisiva nella costruzione del Mercato unico, trovando la propria successiva formalizzazione con l'adozione del *New Legislative Framework* ("NLF")[44].

---

[39] Corte giust., 20 febbraio 1979, causa C-120/78 *Rewe-Zentral AG/Bundesmonopolverwaltung für Branntwein*, ECLI:EU:C:1979:42.

[40] Risoluzione del Consiglio, del 7 maggio 1985, relativa ad una nuova strategia in materia di armonizzazione tecnica e normalizzazione, in *GUCE* C 136 del 4 giugno 1985, p. 1.

[41] Libro Bianco della Commissione per il Consiglio europeo, *Il completamento del mercato interno*, Milano, 28-29 giugno 1985, COM (85) 310 def.

[42] Tale modello succedeva al cd. "vecchio approccio". A tal proposito, la Commissione europea specifica che: «[i]l vecchio approccio rispecchiava la modalità tradizionale con cui le autorità nazionali formulavano la legislazione tecnica, entrando molto nel dettaglio, di solito motivate da una scarsa fiducia nel rigore degli operatori economici su questioni di sicurezza e sanità pubblica. […] L'unanimità richiesta in questo campo fino al 1986 ha notevolmente rallentato l'adozione della legislazione […]», Commissione europea, *Comunicazione - La guida blu all'attuazione della normativa UE sui prodotti 2022*, (2022/C 247/01), par. 1.1.1. In dottrina v. S. DE VRIES, O. KANEVSKAIA, R. DE JAGER, *Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation*, in *European Papers*, 2023, p. 583 ss.

[43] Le norme armonizzate sono state riconosciute dalla Corte di giustizia quali atti facenti parte del diritto dell'UE, cfr. Corte giust., 5 marzo 2024, causa C-588/21 P, *Public.Resource.Org*, ECLI:EU:C:2024:201.

[44] A. VOLPATO, *Delegation of Powers in the EU Legal System*, Londra, 2024; M. CANTERO GAMITO, C. MARSDEN, *Artificial Intelligence Co-regulation? The Role of Standards in the EU AI Act*, in *International Journal of Law and Information Technology*, 2024, p. 11; G. MAZZINI, S. SCALZO, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts*, in C. CAMARDI (a cura di), *op.cit.*, p. 21.

Il NLF – introdotto dal Regolamento (CE) n. 765/2008[45] e dalla decisione n. 768/2008/CE[46], e poi aggiornato dal Regolamento (UE) 2019/1020[47] – ha consolidato e reso più coerente il *New Approach*, introducendo un più elevato livello di responsabilizzazione degli operatori economici attraverso procedure di controllo interno della produzione (*Internal Production Control*) per i prodotti a rischio limitato (Allegato II, modulo A, decisione 768/2008/CE), e un sistema di vigilanza fondato su un approccio esplicitamente basato sul rischio (art. 11, par. 3, del Regolamento (UE) 2019/1020). In virtù di tale impostazione, il tipo di procedura di valutazione della conformità adottato e l'intensità dei controlli previsti sono proporzionati al livello di rischio che il prodotto può comportare per la salute e la sicurezza, in ossequio al principio di proporzionalità.

È all'interno di questo quadro normativo e metodologico che si inserisce l'*AI Act*, che, sotto tale profilo, viene configurato alla stessa stregua della disciplina sulla sicurezza dei prodotti. Come osservato, infatti, esso regolamenta i "sistemi di IA" intesi quali prodotti indipendenti (*stand-alone*) oppure componenti – anche di sicurezza – integrati fisicamente o funzionalmente in un prodotto (considerando 12). L'art. 79 conferma tale qualificazione, stabilendo che «un sistema di IA che presenta un rischio è inteso come un prodotto che presenta un rischio» ai sensi dell'art. 3, punto 19, del Regolamento (UE) 2019/1020[48].

Non sorprende, pertanto, che il regolamento richiami esplicitamente la disciplina delineata dal NLF (*consideranda* 9 e 46) e ne faccia propri, nel Capo III, i principali strumenti di garanzia, quali l'adozione di standard

[45] Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93, in *GUCE* L 218 del 13 agosto 2008, p. 30.

[46] Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE, in *GUCE* L 218 del 13 agosto 2008, p. 82.

[47] Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la Direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011, in *GUUE* L 169 del 25 giugno 2019, p. 1.

[48] V. sul punto M. ALMADA, N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, in *Common Market Law Review*, 1/2025, p. 87: «The product safety approach selected by the AI Act suggests that the EU lawmakers meant to deal with technical objects, not techniques or disciplines.»

tecnici (art. 40)[49], la valutazione di conformità (art. 43), la certificazione da parte di organismi notificati (art. 44) e la marcatura CE, disciplinata in conformità ai principi generali stabiliti dall'art. 30 del citato Regolamento 765/2008 (art. 48).

Le relazioni tra l'*AI Act* e la normativa sulla sicurezza dei prodotti risultano, dunque, riconducibili non solo ad un rapporto ispirato a criteri di continuità, ma anche connotato in termini di complementarità. Ciò è testimoniato dai due differenti approcci adottati dall'*AI Act*, a seconda che il sistema di IA interessi un prodotto rientrante nel perimetro delle normative di armonizzazione adottate nell'ambito del NLF o ne rimanga, invece, estraneo.

Ai sensi dell'art. 8, par. 2, per i sistemi di IA ad alto rischio che rientrano nelle normative adottate nel quadro NFL ed elencate nell'Allegato I, Sezione A si applicano direttamente i requisiti del citato Capo III, Sezione 2, *AI Act*, per il cui rispetto il legislatore europeo ha previsto un regime coordinato rispetto alla legislazione sulla sicurezza dei prodotti, con l'obiettivo di garantirne la coerenza, evitare duplicazioni e minimizzare gli oneri per gli operatori economici (considerando 64). Tale regime attiene, tra gli altri, alla valutazione di conformità dei sistemi di IA, svolta seguendo la procedura prevista dalla disciplina NFL applicabile e relativa al rispetto degli standard tecnici previsti tanto da quest'ultima quanto dall'*AI Act*; alla competenza dell'organismo notificato, individuata in capo a quello previsto dalla disciplina NFL (art. 43, par. 3); alla dichiarazione di conformità UE, redatta in un'unica versione che attesti la conformità del sistema di IA ad alto rischio ai requisiti dell'*AI Act* e della disciplina NFL (art. 47, par. 3); o, ancora, della vigilanza sul mercato, affidata alle autorità competenti secondo la disciplina NFL[50].

Diversamente, per i sistemi di IA ad alto rischio incorporati in, o coincidenti con, prodotti soggetti alle discipline di armonizzazione adottate secondo il "vecchio approccio" ed elencate nell'Allegato I, Sezione B, il legislatore europeo ha attribuito alla Commissione il potere di modificare tali normative tramite atti delegati o di esecuzione, al fine di

[49] Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence, 22/05/2023.

[50] È questo il caso del citato regolamento 745/2017 in materia di dispostivi medici. Sul tema v. Joint Artificial Intelligence Board and Medical Device Coordination Group Document, *Interplay between the Medical Devices Regulation (MDR) & In vitro Diagnostic Medical Devices Regulation (IVDR) and the Artificial Intelligence Act (AIA)*, AIB 2025-1 MDCG 2025-6.

garantire la coerenza con i requisiti dell'*AI Act* e, al contempo, rispettare le specificità tecniche di ciascuna di esse (considerando 49). Pertanto, ai sensi dell'art. 2, par. 2, *AI Act*, i citati requisiti tecnici del Capo III, Sezione 2 non si applicano a tali sistemi fino all'adozione di tali atti delegati o di esecuzione da parte della Commissione, in forza dei poteri conferiti dagli artt. 102-110 *AI Act*.

Questo impianto normativo specifico dell'*AI Act* non implica che i sistemi di intelligenza artificiale non ad alto rischio, collegati a prodotti, restino privi di disciplina. Essi, infatti, continuano a essere regolati da strumenti orizzontali di tutela, quali, ad esempio, la normativa generale sulla sicurezza dei prodotti (Regolamento (UE) 2023/988[51]) e la legislazione in materia di protezione dei dati personali (*consideranda* 166 e 10 *AI Act*).

2.1.2. …e di discontinuità

Se, dunque, un significativo punto di riferimento normativo del *risk-based approach* previsto dal regolamento può essere individuato nella disciplina europea sulla sicurezza dei prodotti, di contro, l'esplicito riconoscimento della tutela dei diritti fondamentali rappresenta un elemento di discontinuità rispetto all'impostazione precedente. È, peraltro, quanto emerge dalla scelta della Commissione, già in fase di proposta, di prevedere una duplice base giuridica del regolamento che, difatti, non si fonda solo sull'art. 114 TFUE relativo all'armonizzazione del mercato interno, ma anche sull'art. 16 TFUE dedicato alla protezione dei dati personali[52].

Tale discontinuità, tuttavia, non ha carattere assoluto. Infatti, il legislatore dell'UE è tenuto al rispetto dei diritti fondamentali nell'esercizio delle competenze conferitegli dai Trattati anche quando interviene in materia di sicurezza dei prodotti, come confermato, in più

[51] Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio del 10 maggio 2023 relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la Direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la Direttiva 87/357/CEE del Consiglio, in *GUUE* L 135 del 23 maggio 2023, p. 1.

[52] S. POLI, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE*, 5/2021, p. 69; T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno. Riflessioni sul sistema delle fonti alla luce dell'art. 114 TFUE*, Bari, 2018.

occasioni, dalla Corte di giustizia[53]. È il caso, ad esempio, del Regolamento (UE) 2017/745 sui dispositivi medici che prevede esplicitamente la tutela dei diritti fondamentali sebbene si tratti di una normativa incardinata nel NFL[54].

Ciononostante, a differenza degli altri atti in materia di sicurezza dei prodotti, per l'*AI Act* il rispetto dei diritti fondamentali è posto sullo stesso

[53] La giurisprudenza della Corte di giustizia, in più occasioni, ha ribadito la necessità di tutelare i diritti fondamentali anche nell'ambito dell'armonizzazione finalizzata alla realizzazione del mercato unico. Ad esempio, nella sentenza *Omega*, la Corte ha riconosciuto che «il rispetto dei diritti fondamentali si impone (…) sia alla Comunità sia ai suoi Stati membri» e, pertanto, «la tutela di tali diritti rappresenta un legittimo interesse che giustifica, in linea di principio, una limitazione degli obblighi imposti dal diritto comunitario, ancorché derivanti da una libertà fondamentale garantita dal Trattato quale la libera prestazione dei servizi», Corte giust., 14 ottobre 2004, causa C-36/02, *Omega*, ECLI:EU:C:2004:614, punto 35. Analogamente, nella causa *Schmidberger*, il giudice dell'Unione ha affermato che la libera circolazione delle merci può essere limitata per garantire l'esercizio di diritti fondamentali quali la libertà di espressione e di riunione, sottolineando la necessità di un bilanciamento proporzionato tra libertà economiche e diritti fondamentali, Corte giust., 12 giugno 2003, causa C-112/00, *Schmidberger*, ECLI:EU:C:2003:333, punti 74-81. Infine, nella causa *Polonia v. Parlamento e Consiglio*, la Corte ha specificato che: «qualora più diritti fondamentali e principi sanciti dai Trattati siano in discussione, la valutazione del rispetto del principio di proporzionalità deve essere effettuata nel rispetto della necessaria conciliazione tra le esigenze connesse alla tutela dei diversi diritti e principi in questione e di un giusto equilibrio tra di essi», Corte giust., 26 aprile 2022, causa, C-401/19, *Polonia v. Parlamento e Consiglio*, ECLI:EU:C:2022:297, punto 66. A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *I Post di AISDUE*, 15/2023, p. 325; B. NASCIMBENE, *Carta dei Diritti Fondamentali, applicabilità e rapporti fra Giudici. La necessità di una tutela integrata*, in C. AMALFITANO, M. D'AMICO, S. LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione europea nel sistema integrato di tutela*, Torino, 2022, p. 37; A. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pisa, 2020, p. 13.

[54] All'espresso riferimento alla libertà di stampa, quale valore da salvaguardare nell'attuazione del regolamento ai sensi dell'art. 1, par. 16, si sommano le previsioni di cui agli artt. 33, par. 7 e l'art 62, par. 4, lett. h. La prima, relativa alla cd. Banca dati europea dei dispositivi medici, stabilisce l'obbligo per la Commissione e gli Stati membri di garantire alle persone interessate l'esercizio effettivo dei diritti conferiti loro dalla disciplina in materia di protezione dei dati personali (diritti di informazione, di accesso e di rettifica). La seconda, invece, prevede che le indagini cliniche debbano rispettare «il diritto all'integrità fisica e mentale del soggetto, il diritto alla riservatezza e alla protezione dei dati che lo riguardano». Infine, come precisato dal considerando 89, il regolamento 745/2017 «rispetta i diritti fondamentali e i principi riconosciuti, in particolare, dalla Carta e, segnatamente, la dignità umana, l'integrità della persona, la protezione dei dati di carattere personale, la libertà delle arti e delle scienze, la libertà d'impresa e il diritto di proprietà»; diritti e principi che – aggiunge il considerando – gli Stati membri dovrebbero osservare nell'applicazione del regolamento.

piano della salute e della sicurezza, assumendo, di fatto, il ruolo di principale criterio di classificazione dei sistemi di IA (*consideranda* 9 e 48)[55]. A conferma di ciò, l'art. 7 prevede che la Commissione possa aggiornare, mediante atti delegati, l'elenco dei sistemi di IA ad alto rischio di cui al citato Allegato III, proprio al fine di tenere conto dei «rischi significativi per la salute, la sicurezza o i diritti fondamentali» delle persone. In modo analogo, l'art. 9, par. 2, nel disciplinare il sistema di gestione del rischio, impone ai fornitori di identificare, analizzare e mitigare non solo i rischi per la salute e la sicurezza, ma anche quelli per i diritti fondamentali, trattandoli su un piano di pari rilevanza, quali "interessi pubblici"[56].

La centralità attribuita dal regolamento ai diritti fondamentali trova una propria giustificazione secondo una duplice prospettiva: da un lato, si pone in linea con il rilievo assunto da tali diritti nell'evoluzione del settore digitale dell'UE e, dall'altro lato, è legata alle specifiche caratteristiche dei sistemi di intelligenza artificiale.

La prima prospettiva è di ordine sistematico. L'*AI Act* si colloca, infatti, nella seconda fase della politica dell'UE per il digitale, avviata dalla Commissione una volta completata la Strategia per il Mercato Unico Digitale[57]. Tale strategia è stata contraddistinta – trasversalmente ai suoi tre pilastri «migliore accesso dei consumatori e delle imprese ai beni e servizi digitali in tutta Europa», «creare un contesto favorevole affinché le reti e i servizi digitali possano svilupparsi» e «massimizzare il potenziale di crescita dell'economia digitale» – da un approccio prevalentemente

[55] Sul tema dei diritti fondamentali nell'*AI Act* si rimanda a F. DONATI, *La protezione dei diritti fondamentali nel Regolamento sull'Intelligenza Artificiale*, in *Rivista Associazione Italiana Costituzionalisti*, 1/2025, p. 1; A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: brevi considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *op.cit.*, p. 127; G. SARTOR, *Artificial Intelligence and Human Rights: Between Law and Ethics*, in *Maastricht Journal of European and Comparative Law*, 2020, p. 705.

[56] Cfr. considerando n. 7, secondo cui: «[a]l fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali […]». M. ALMADA, N. PETIT, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, in *Robert Schuman Centre for Advanced Studies - Working Paper*, 2023, p. 17.

[57] Commissione europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 def. V. B. NASCIMBENE, *Il mercato unico digitale è una nuova frontiera dell'integrazione europea?*, in *Eurojus*, 3/2025, p. 105.

economico, volto a creare un ecosistema favorevole allo sviluppo delle infrastrutture tecnologiche e dei servizi online[58].

Con il passaggio alla suddetta seconda fase della politica dell'UE per il digitale, gli Orientamenti politici per la Commissione europea 2019-2024 hanno individuato come priorità la realizzazione di «[u]n'Europa pronta per l'era digitale», espressione che rivela, pur a fronte della precedente intensa attività legislativa, la consapevolezza di una parziale inadeguatezza dell'ordinamento dell'UE rispetto ai rischi e alle sfide posti dalla trasformazione digitale. In tale contesto, la comunicazione *Plasmare il futuro digitale dell'Europa*[59] ha segnato un mutamento di approccio, ponendo tre obiettivi cardine – «una tecnologia a servizio delle persone», «un'economia equa e competitiva» e «una società aperta, democratica e sostenibile» – accomunati, come evidente già dalla loro denominazione, dall'intento di guidare tale transizione digitale attraverso i valori e la tutela dei diritti fondamentali[60]. La nuova politica digitale europea, in attuazione del principio sancito dall'art. 3, par. 3 TUE, si è indirizzata ad un modello di «economia sociale di mercato fortemente competitiva» che trova effettiva concretizzazione, a livello dell'*AI Act*, nella centralità attribuita alla tutela dei diritti fondamentali[61].

La seconda prospettiva, invece, è di ordine sostanziale e riguarda la natura stessa dei sistemi di IA. Come chiarito dalla definizione contenuta nell'art. 3, punto 1, *AI Act*, essi si distinguono dai *software* e dagli algoritmi tradizionali per la combinazione di autonomia e di capacità inferenziale[62].

---

[58] F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il Regolamento UE sulla privacy*, in R. CAVALLO PERIN, D.-U. GALETTA (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, 2025, p. 43.

[59] Commissione europea, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 def.

[60] C. AMALFITANO, F. FERRI, *Transizione digitale e dimensione costituzionale dell'Unione europea: tra principi, diritti e valori*, in R. TORINO, S. ZORZETTO (a cura di), *La trasformazione digitale in Europa. Diritti e principi*, Torino, 2023, p. 1.

[61] Sul concetto di "economia sociale di mercato fortemente competitiva", v. G. CONTALDI, *Il significato attuale dell'economia sociale di mercato nell'ordinamento dell'Unione europea*, in *Ordine internazionale e diritti umani*, 2018, p. 544.

[62] Il considerando 12 *AI Act* si riferisce alla capacità inferenziale quale «caratteristica fondamentale dei sistemi di IA». Inoltre, la Commissione europea precisa che la capacità inferenziale è strettamente connessa all'adattabilità che è necessaria, quantomeno in un certo grado, perché un sistema di IA possa definirsi tale, v. European Commission, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, cit., para. 15.

L'autonomia designa la possibilità del sistema di disporre "*di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano*"[63].

La capacità inferenziale, invece, consiste nell'attitudine del sistema a dedurre e generare, dagli *input* ricevuti, risultanze in grado di alterare l'ambiente, fisico o digitale, circostante[64]. Tale capacità è attuata grazie all'impiego di tecniche di *machine learning* e *deep learning*, che consentono al sistema di IA di evolvere, durante l'uso, in base alle sue esperienze[65].

L'intelligenza artificiale, pertanto, incidendo sui principi della sorveglianza umana e della trasparenza, espone un numero ampio ed eterogeneo di diritti fondamentali ad un livello di rischio accentuato[66].

Il *risk-based approach* dell'*AI Act* e la relativa classificazione dei sistemi di intelligenza artificiale rappresentano, dunque, un'evoluzione del paradigma di sicurezza dei prodotti: originariamente volto a bilanciare tra loro la libertà di circolazione e la sicurezza, una volta trasposto nel dominio digitale, tale approccio ha assunto una connotazione "valoriale" che ruota sull'impatto del prodotto-sistema di IA sui diritti fondamentali dell'UE.

---

[63] European Commission, *Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act)*, cit., para. 14-21.
[64] *Ibid.*, parr. 26-29.
[65] *Ibid.*, parr. 30-39.
[66] Crf. considerando 48 in cui l'*AI Act* cita espressamente il diritto alla dignità umana (articolo 1), al rispetto della vita privata e alla protezione dei dati di carattere personale (articoli 7 e 8), alla non discriminazione (articolo 21) e alla parità tra donne e uomini (articolo 23) alla libertà di espressione (articolo 11), alla libertà di riunione (articolo 12), nonché ad assicurare la tutela del diritto a un ricorso effettivo e a un giudice imparziale, della presunzione di innocenza e dei diritti della difesa (articoli 47 e 48), così come il principio generale di buona amministrazione, il diritto a un livello elevato di tutela dell'ambiente e al miglioramento della sua qualità (articolo 37) e, infine, i diritti relativi a gruppi speciali, quali i diritti dei lavoratori a condizioni di lavoro giuste ed eque (articolo 31), un livello elevato di protezione dei consumatori (articolo 38), i diritti del minore (articolo 24 e Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, e persone con disabilità (articolo 26).

3. L'approccio basato sul rischio dell'*AI Act* e la disciplina sulla protezione dei dati personali: profili di continuità e discontinuità

3.1. L'approccio basato sul rischio nella disciplina sulla protezione dei dati personali

L'approccio basato sul rischio adottato dall'*AI Act* costituisce un elemento di continuità rispetto non solo all'ambito normativo NFL, bensì anche all'*aquis communitaire* in materia di protezione dei dati personali e, nello specifico, al Regolamento (UE) 2016/679 ("GDPR")[67]. Sebbene il GDPR non fornisca una definizione espressa del termine "rischio", l'articolato normativo è permeato dalla logica del *risk-based approach*[68], in continuità con la traiettoria già tracciata dalla Direttiva 95/46/CE[69]. Difatti, come evidenziato dal Gruppo Articolo 29 (oggi sostituito dal cd. Comitato europeo per la protezione dei dati o "EDPB"), l'approccio basato sul rischio, inteso come «approccio scalabile e proporzionato alla conformità», ha caratterizzato la Direttiva 95/46/CE, segnatamente in tema

---

[67] 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), in *GUUE* L 119 del 4 maggio 2016, p. 1. Per una prima introduzione alla normativa in materia di protezione dei dati personali v. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *Commentario GDPR e Normativa Privacy*, Milano, 2022; F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *op.cit.*, p. 43 ss.; R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e* data protection, Milano, 2021; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017.

[68] Sul punto v. Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal Frameworks*, 30 maggio 2014, 14/EN WP 218, p. 2, secondo cui: «the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation. It has been introduced recently as a core element of the accountability principle itself». In dottrina v. A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, in *Computer Law & Security Review*, 2024, p. 2; R. GELLERT, *Understanding the notion of risk in the General Data Protection Regulation*, in *Computer Law & Security Review*, 2018, p. 279; D. LEUFER, F. HIDVEGI, A. ZORNETTA, *The Pitfalls of the European Union's Risk-Based Approach to Digital Rulemaking*, cit. p. 162 ss.

[69] 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, in *GUCE* L 281 del 23 novembre 1995, p. 31.

di sicurezza del trattamento (art. 17) e di controllo preventivo da parte dell'autorità di controllo (art. 20)[70].

Partendo da questo presupposto, il Regolamento sulla protezione dei dati personali ha elevato il *risk-based approach* a fondamento di uno dei suoi principi cardine, ossia quello di responsabilizzazione ("*accountability*")[71], secondo cui è il titolare del trattamento che è chiamato, in quanto «*responsabile*» (art. 5, par. 2 e considerando 74, GDPR)[72], a garantire e comprovare la legittimità del trattamento mediante l'adozione di misure tecniche e organizzative (art. 24, par. 1, GDPR). A tal fine, esso specifica che queste misure devono basarsi su di una «*valutazione oggettiva*" che tenga da conto «dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche» quali, ad esempio, «discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo» (*consideranda* 75 e 76 GDPR).

Il *risk-based approach* si riflette, altresì, sull'obbligo di cui all'art. 33 del GDPR in materia di violazione dei dati personali ("*data breach*"). Il titolare del trattamento, infatti, è tenuto a valutare se tale violazione possa determinare «un rischio per i diritti e le libertà delle persone fisiche», ipotesi ricorrente in caso esse possano subire un «danno fisico, materiale o immateriale» (*consideranda* 87 e 88 GDPR). Da tale rischio discende, in capo al titolare, il duplice obbligo di notifica all'autorità di controllo nazionale competente – ovvero, nel caso la violazione presenti carattere transfrontaliero all'autorità capofila individuata ai sensi del meccanismo di cooperazione – e, qualora il rischio stesso sia "notevole", di estendere la comunicazione direttamente agli interessati. Tali obblighi di notifica, tuttavia, non trovano applicazione se il titolare è in grado di dimostrare, in conformità al principio di responsabilizzazione, che la violazione è

[70] Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal Frameworks*, cit., p. 2.
[71] T. STREINZ, *The Evolution of European Data Law*, in P. CRAIG, G. DE BÚRCA (a cura di), *The Evolution of EU Law*, Oxford, 2021; R. GELLERT, *The Risk-Based Approach to Data Protection*, Oxford, 2020, p. 27.
[72] Si tratta dei principi di "liceità, correttezza e trasparenza", "limitazione della finalità", "minimizzazione dei dati", "esattezza", "limitazione della conservazione", "integrità e riservatezza", stabiliti dall'art. 5, par. 1 GDPR. Sul tema v. Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 13 luglio 2010, 00062/10/EN WP 173.

«improbabile che comporti un rischio per i diritti e le libertà delle persone fisiche coinvolte»[73].

Infine, come si avrà modo di osservare in seguito, una simile ponderazione è rimessa al titolare dall'art. 35, par. 1, GDPR che gli impone di valutare preventivamente l'impatto, anche solo potenziale, dei trattamenti che presentino «un rischio elevato per i diritti e le libertà delle persone fisiche»[74].

3.2. L'approccio basato sul rischio: il confronto tra GDPR e *AI Act*

Sebbene, quindi, l'approccio basato sul rischio costituisca uno strumento cardine tanto per l'*AI Act* quanto per il GDPR, la dottrina ha messo in luce alcune differenze[75].

Nello specifico, nel GDPR la valutazione dei rischi e la scelta dei relativi interventi di mitigazione non sono predeterminate in maniera rigida dal legislatore, rientrando, invece, nella responsabilità del titolare del trattamento, che deve calibrare le misure tecniche e organizzative alla natura, all'ambito di applicazione, al contesto, alle finalità e ai rischi dello specifico trattamento dei dati personali.

Tale regolamento fissa una soglia di "rischio elevato" superata la quale il principio di responsabilizzazione cede il posto all'applicazione di

---

[73] EDPB, *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679*, 3 ottobre 2017, 18/IT WP250rev.01.

[74] *Ivi*, par. 104, in merito al rapporto tra le valutazioni da svolgersi ai sensi degli artt. 33 e 35: «Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati. Quest'ultima considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, esamina in termini generali la probabilità che la stessa si verifichi e il danno all'interessato che potrebbe derivarne; in altre parole, si tratta di una valutazione di un evento ipotetico. Nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.»

[75] D. LEUFER, F. HIDVEGI, A. ZORNETTA, *The Pitfalls of the European Union's Risk-Based Approach to Digital Rulemaking*, cit, p. 162, che fa riferimento al GDPR come ad una normativa che adotta un "right-based approach" con elementi tipici del "risk-based approach"; M. ALMADA, N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, cit., p. 96, secondo cui: «The overall picture brings the AI Act closer to market-oriented instruments such as the Digital Markets Act than to fundamental rights instruments such as the General Data Protection Regulation (GDPR).» Sul tema v. anche R. GELLERT, *The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's Proposed Artificial Intelligence Act: Business as Usual?*, in *Journal of Ethics and Legal Technologies*, 3/2021, p. 15.

obblighi sostanziali o procedurali, quali il coinvolgimento dell'autorità competente ai sensi dei suddetti artt. 33 e 35. Tuttavia, tale soglia non è stabilita dalla normativa stessa, bensì dal titolare, in base ad un bilanciamento degli interessi e dei rischi in gioco. Il risultato è un approccio flessibile che, individuando obiettivi generali e lasciando ampi margini di discrezionalità, integra una dinamica regolatoria del tipo "*bottom-up*"[76].

Diversamente, l'*AI Act*, come osservato, utilizza il concetto di rischio quale strumento di valutazione e classificazione dei sistemi di IA, da cui deriva l'applicazione di requisiti più o meno stringenti. Infatti, pur prevedendo obblighi graduati e proporzionati, l'approccio basato sul rischio in questo contesto non attribuisce ai fornitori o ai *deployer* il potere di determinare in autonomia la pericolosità associata ad un sistema di IA, essendo questa prefissata in via autoritativa. È il legislatore a identificare *ex lege* le citate quattro categorie di rischio e a stabilire per ciascuna le corrispondenti conseguenze giuridiche. Ne consegue che la discrezionalità intrinseca alla valutazione del rischio, centrale nel GDPR, è sostituita nel Regolamento sull'AI da una tassonomia di matrice legislativa, in una dinamica regolatoria del tipo "*top-down*"[77].

Queste distinzioni, valide sul piano teorico, tuttavia, si attenuano sensibilmente sul piano applicativo, segnatamente sotto i profili dell'imposizione dei divieti, della tutela rafforzata verso specifiche categorie di soggetti "vulnerabili" e dell'istituzione di appositi sistemi di gestione del rischio[78].

---

[76] Cfr. G. DE GREGORIO, P. DUNN, *European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 2022, p. 478; A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, cit., p. 4; S. DELACROIX, N.D. LAWRENCE, *Bottom-up data Trusts: disturbing the 'one size fits all' approach to data governance*, in *International Data Privacy Law*, 9/2019, p. 236.

[77] Cfr. M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, cit., p. 195 ss.; M. ALMADA, N. PETIT, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, cit., p. 8; G. DE GREGORIO, P. DUNN, *European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, cit., p. 489.

[78] R. GELLERT, *The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual?*, cit., p. 24. Per una panoramica sulle interazioni tra GDPR e intelligenza artificiale v. G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence - Panel for the Future of Science and Technology – (EPRS) European Parliamentary Research Service*, PE 641.530 – June

3.2.1. Il primo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: l'imposizione dei divieti

Un primo punto di contatto tra l'approccio basato sul rischio del GDPR e quello dell'*AI Act* risiede nell'imposizione di divieti che riducono gli spazi di discrezionalità degli operatori, secondo una logica *top-down*.

In tal senso, l'art. 5, par. 1, *AI Act* vieta la messa sul mercato e l'utilizzo dei sistemi di IA qualificati come a rischio inaccettabile, mentre l'art. 9, par. 1, GDPR proibisce il trattamento delle categorie particolari di dati personali[79]. In entrambe le ipotesi il legislatore europeo predefinisce soglie di rischio oltre le quali l'attività non è consentita, circoscrivendo i margini di azione dei fornitori e dei *deployer*, da un lato, e dei titolari del trattamento, dall'altro.

Il fatto che l'art. 9, par. 2, GDPR preveda un catalogo di esenzioni al relativo divieto non incrina tale parallelismo, giacché anche il Regolamento sull'IA contempla deroghe specifiche ai divieti imposti ai sistemi a rischio inaccettabile. Tali deroghe dell'*AI Act* appaiono, peraltro, concettualmente riconducibili alla disciplina in materia di protezione dei dati personali con ciò segnando un ulteriore punto di contatto tra le due discipline.

Nello specifico, l'art. 5, par. 1, lett. *d)*, *AI Act* vieta i sistemi di IA destinati a «valutare o prevedere il rischio» che una persona commetta un reato, unicamente sulla base – per quanto qui interessa – della sua «profilazione»[80]. Il divieto non trova, tuttavia, applicazione nel caso ricorrano due condizioni cumulative: (*i*) i sistemi di IA siano «utilizzati a sostegno della valutazione umana»; (*ii*) i sistemi di IA si fondino «su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa»[81].

2020. A. WERNICK, *Impact Assessment as a Legal Design Pattern - A "Timeless Way" of Managing Future Risks?*, in *Digital Society* 3/2024, p. 29; C.D. RAAB, *Information Privacy, Impact Assessment, and the Place of Ethics*, in *Computer Law & Security Review*, 2020, p. 1.

[79] V. Article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal Frameworks*, cit., p. 2: «The legal regime applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach: strengthened obligations result from processing which is considered risky for the persons concerned.»

[80] Oltre alla profilazione la norma vieta la valutazione o previsione fondata sui tratti della personalità e delle caratteristiche, quali cittadinanza, residenza, luogo di nascita, composizione famigliare, condizioni economiche, ecc. (considerando 42, *AI Act*).

[81] European Commission, *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, cit., punti 203 ss.

Con riguardo alla prima condizione, in sostanza, l'*AI Act* richiede l'intervento umano[82] quale elemento di frapposizione al funzionamento completamente automatizzato del sistema di IA, tipico delle tecniche di profilazione[83]. L'importanza di tale intervento umano deriva dalla tradizione normativa in materia di *privacy* che lo interpreta quale fattore di attenuazione dei rischi. A dimostrazione di ciò può farsi riferimento all'art. 22 GDPR, il quale vieta le decisioni basate unicamente sul trattamento automatizzato, ivi compresa la profilazione, qualora producano "effetti giuridici", o comunque "significativi", per l'interessato (par. 1), a meno che quest'ultimo non abbia avuto la possibilità di esercitare il suo diritto di ottenere un intervento umano, esprimere la propria opinione e contestare siffatta decisione (par. 2)[84]. Analogamente, la Direttiva (UE) 2016/680 relativa alla tutela della privacy nell'ambito dell'attività di contrasto (cd. Direttiva LED)[85] vieta le decisioni interamente automatizzate con effetti pregiudizievoli, esclusi i soli casi in cui essa si fondi sul diritto dell'Unione o nazionale e preveda, anche in

[82] Il concetto di "intervento umano" è da intendersi sulla scorta della giurisprudenza della Corte di giustizia quale, ad esempio, la sentenza del 21 giugno 2022, causa C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:491.

[83] Il concetto di "profilazione" di cui all'art. 3, punto 52 dell'*AI Act* è definito in termini corrispondenti a quanto stabilito dall'art. 4, punto 4, del GDPR e dall'art. 3, punto 4, della Direttiva LED. V. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* WP251rev.01, 6.2.2018. Per un approfondimento sulla profilazione v. A. ADINOLFI, A. SIMONCINI (a cura di), *Protezione dei dati personali, e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli, 2022; Agenzia dell'Unione europea per i diritti fondamentali, *Evitare la profilazione illecita oggi e in futuro: una guida,* Lussemburgo, 2019; 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*, 7/2017, p. 76; I. MENDOZA, L.A. BYGRAVE, *The Right Not to Be Subject to Automated Decisions Based on Profiling*, in T.-E. SYNODINOU, P. JOUGLEUX, C. MARKOU, T. PRASTITOU (a cura di), *EU Internet Law: Regulation and Enforcement*, 2017, Cham, p. 77; L. EDWARDS, M. VEALE, *Slave to the Algorithm? Why a «Right to Explanation» is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, 2017, p. 32.

[84] V. considerando 71, GDPR. Sul tema la Corte di giustizia ha già avuto modo di evidenziare, in più occasioni, la pericolosità delle tecniche di trattamento dei dati personali automatizzate, cfr. Corte giust., 16 luglio 2020, C-311/18, *Schrems I*, EU:C:2020:559, punto 176.

[85] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, in *GUUE* L *119 del 4 maggio 2016, p. 89.*

questo caso, garanzie adeguate per i diritti e le libertà dell'interessato (art. 11, par. 1).

Pertanto, in linea con la logica del GDPR e della Direttiva LED, l'*AI Act* richiede una forma di controllo e supervisione umana al fine di limitare i rischi di discriminazione associati al funzionamento totalmente automatizzato di tecniche di cd. *predictive policing*[86].

In merito alla seconda condizione relativa al concetto di «fatti obiettivi e verificabili», essa trova corrispondenza nel principio di esattezza dei dati sancito dall'art. 5, par. 1, lett. d), GDPR, secondo cui i dati personali devono essere «esatti e, se necessario, aggiornati», dal titolare che, a tal fine, deve adottare «misure ragionevoli per cancellare o rettificare tempestivamente» eventuali incongruità. In parallelo, l'art. 7 della Direttiva LED impone agli Stati membri di distinguere tra dati personali basati su fatti e quelli fondati su valutazioni soggettive, garantendo che i dati inesatti, incompleti o obsoleti non siano né trasmessi né resi disponibili, e assicurando che le autorità competenti verifichino la qualità dei dati in fase di reciproca comunicazione. Sia il principio di esattezza del GDPR sia gli obblighi di qualità dei dati sanciti dalla Direttiva LED appaiono, dunque, anticipare i requisiti di obiettività e verificabilità previsti dall'eccezione di cui all'art. 5, par. 1, lett. d), dell'*AI Act*.

3.2.2. Il secondo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: la tutela rafforzata dei soggetti vulnerabili

Un secondo punto di convergenza tra l'approccio basato sul rischio dell'*AI Act* e quello del GDPR emerge nella previsione di forme di tutela rafforzata nei confronti dei soggetti vulnerabili, le quali, anche in questo caso, contribuiscono a ridurre la responsabilizzazione degli operatori, secondo una logica regolatoria di tipo *top-down*.

In particolare, l'art. 5, par. 1, lett. a) e b), *AI Act* vieta l'uso di sistemi di IA che sfruttino le vulnerabilità di determinati gruppi di persone, quali minori, anziani, persone con disabilità o in condizioni economiche svantaggiate. Il divieto mira a prevenire pratiche manipolative o subliminali che, facendo leva sull'asimmetria cognitiva tipica di tali categorie e sulla forza persuasiva degli *output* generati dall'IA, rischiano di compromettere i diritti fondamentali quali la dignità, l'autonomia

[86] G. BARONE, *Giustizia predittiva e certezza del diritto*, cit., p. 47; S. LONATI, Predictive policing*: dal disincanto all'urgenza di un ripensamento*, in *MediaLaws - Rivista di diritto dei media*, 2/2022, p. 302.

decisionale e il principio di non discriminazione, espressamente tutelati dagli artt. 1 e 21 della Carta dei diritti fondamentali dell'UE (considerando 29, *AI Act*)[87]. A ciò si aggiunge l'art. 9, par. 9, *AI Act*, che, nell'ambito del citato sistema di gestione dei rischi, impone ai fornitori di considerare la possibilità che i sistemi di IA ad alto rischio producano effetti negativi sui minori di diciotto anni o, se del caso, su altri gruppi vulnerabili, integrando così un obbligo specifico di valutazione *ex ante* della loro condizione di fragilità.

Un'impostazione concettualmente analoga si rinviene nel GDPR. L'art. 8 prevede infatti una protezione rafforzata per i minori in relazione al trattamento dei dati personali nell'ambito dei servizi della società dell'informazione, subordinando la validità del consenso alla soglia anagrafica dei sedici anni, salvo che gli Stati membri stabiliscano un'età inferiore, purché non al di sotto dei tredici anni[88]. Inoltre, la disciplina della profilazione nei confronti dei minori è oggetto di un divieto espresso, come chiarito dall'art. 22, par. 1, GDPR, al fine di impedire trattamenti automatizzati suscettibili di produrre effetti giuridici o comunque significativi nei loro confronti (considerando 71)[89].

Tanto nell'*AI Act* quanto nel GDPR emerge dunque una comune *ratio*, volta a garantire che la gestione del rischio non trascuri la condizione di vulnerabilità di determinati soggetti, la quale, proprio per la sua rilevanza assiologica, costituisce un limite alla discrezionalità degli operatori economici.

---

[87] European Commission, *Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*, cit., para. 58 ss.

[88] Ai sensi dell'art. 8, par. 1, è fatta salva la possibilità per gli Stati membri di fissare tale soglia ad un'età inferiore, purché non al di sotto dei tredici anni (considerando 38). Sul tema della tutela dei minori ai sensi del GDPR, v. C. CAGLAR, *Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?*, in *European Journal of Law and Technology*, 2/2021, p. 1.

[89] Tale divieto posto dal GDPR è stato ulteriormente rinforzato tramite la previsione, nel citato *Digital Service Act*, dell'art. 28, par. 2 che vieta ai fornitori di piattaforme online di presentare sulla loro interfaccia pubblicità basata sulla profilazione che usa i dati personali del destinatario del servizio nel caso in cui, con ragionevole certezza, il destinatario del servizio sia un minore. Sull'interazione dei divieti posti dal GDPR e dal DSA la Commissione è intervenuta il 10 ottobre 2025 con gli *Orientamenti su misure per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori online, a norma dell'articolo 28, paragrafo 4, del regolamento (UE) 2022/2065*, (C/2025/5519).

3.2.3. Il terzo parametro di analogia tra l'approccio basato sul rischio dell'*AI Act* e del GDPR: la gestione del rischio

Le analogie sostanziali tra l'approccio basato sul rischio adottato dall'*AI Act* e quello sotteso al GDPR riguardano altresì la prospettiva *bottom-up*, nel segno di previsioni che valorizzano la responsabilizzazione tanto dei titolari, ai sensi del GDPR, quanto dei fornitori e dei *deployer*, ai sensi dell'*AI Act*.

Si collocano in questo ambito l'art. 9 *AI Act*, che impone ai fornitori l'adozione del sistema di gestione dei rischi (*Risk Management System*, "RMS"), e l'art. 27, che introduce l'obbligo di una valutazione d'impatto sui diritti fondamentali (*Fundamental Rights Impact Assessment*, "FRIA"). Entrambi gli strumenti mostrano evidenti punti di contatto con l'art. 35 GDPR relativo alla valutazione d'impatto sulla protezione dei dati (*Data Protection Impact Assessment*, "DPIA")[90].

Prima, tuttavia, di analizzare le analogie tra detti strumenti è opportuno esaminarli partitamente.

L'art. 9 *AI Act* impone ai fornitori di sistemi di IA ad alto rischio l'obbligo di istituire, attuare, documentare e mantenere un sistema di gestione dei rischi (par. 1), qualificato come un «processo iterativo continuo», soggetto a costante aggiornamento e «pianificato ed eseguito lungo l'intero ciclo di vita» del sistema stesso (par. 2). Il processo si articola in tre fasi. La prima consiste nell'identificazione e nell'analisi dei rischi che l'utilizzo di tale sistema ad alto rischio può comportare per la salute, la sicurezza e i diritti fondamentali delle persone. In tale ambito rientrano i rischi noti, quelli ragionevolmente prevedibili – anche da usi impropri del sistema – nonché quelli individuati attraverso l'analisi dei dati raccolti dal monitoraggio successivo all'immissione sul mercato ai sensi dell'art. 72 *AI Act*. La seconda fase concerne la stima e la valutazione dei rischi individuati. Infine, la terza implica l'adozione delle misure di gestione e di mitigazione più adeguate «alla luce dello stato dell'arte in materia di IA» (considerando 65), allo scopo di ridurre i rischi individuati e valutati a un livello ritenuto «*accettabile*», attraverso misure tecniche (ad

[90] A. COSENTINI ET AL., *Assessing the Impact of Artificial Intelligence Systems on Fundamental Rights*, in *MediaLaws - Rivista di Diritto dei Media*, 2025, p. 1; S. BERTAINA ET AL., *Fundamental rights and artificial intelligence impact assessment: A new quantitative methodology in the upcoming era of AI Act*, in *Computer Law & Security Review*, 2025, p. 1; A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, cit., p. 2; A. WERNICK, *Impact Assessment as a Legal Design Pattern - A "Timeless Way" of Managing Future Risks?*, in *Digital Society*, 3/2024, p. 29.

es. cibersicurezza e *compliance by design* e *by default*) e organizzative (ad es. formazione dei *deployer*)[91].

L'art. 27 *AI Act* prevede l'obbligo di effettuare la FRIA che, a differenza del RMS, non grava sui fornitori, bensì esclusivamente su determinate categorie di *deployer*. Da un lato, esso riguarda gli organismi di diritto pubblico e gli enti privati che erogano servizi pubblici, con l'eccezione di quelli operanti nel settore delle infrastrutture critiche di cui all'Allegato III, punto 2. Dall'altro lato, si applica ai *deployer* che utilizzano sistemi di IA ad alto rischio individuati all'Allegato III, punto 5, lett. b) e c), rispettivamente destinati alla valutazione dell'affidabilità creditizia – con esclusione dei sistemi impiegati per la rilevazione di frodi finanziarie – e allo *scoring* a fini assicurativi nel settore delle polizze vita e salute.

Ai sensi dell'art. 27 *AI Act*, tali *deployer* sono tenuti a predisporre un sistema strutturato di valutazione e mitigazione dei rischi, analogo al RMS previsto per i fornitori dall'art. 9. Tuttavia, a differenza di quest'ultimo, in cui la tutela dei diritti fondamentali rappresenta soltanto uno degli elementi considerati nella valutazione complessiva dei rischi, la FRIA si configura quale strumento specificamente orientato alla loro protezione.

Attraverso il duplice obbligo di instaurare il sistema RMS, in capo ai fornitori, e di effettuare la FRIA, in capo ai *deployer*, l'*AI Act* istituisce una disciplina di gestione del rischio che interessa la maggior parte della catena di produzione di valore associata ai sistemi di IA. L'onere della gestione del rischio è così ripartito in modo proporzionale tra i due soggetti, in funzione sia della tipologia di pericolo generato, sia del rispettivo grado di controllo esercitabile sul sistema. Difatti, la circostanza, già osservata, che i rischi connessi ai sistemi di IA non dipendono unicamente dalle loro caratteristiche progettuali, ma possono emergere anche dalle modalità concrete di impiego, pone i *deployer* nella posizione migliore per individuare rischi residuali o nuovi profili di criticità non intercettati in fase di sviluppo, assumendo un ruolo così decisivo nella salvaguardia dei diritti fondamentali (considerando 93 e 96). A tal fine, la disciplina stabilisce uno specifico flusso informativo tra le due categorie di soggetti che si attua mediante la redazione, da parte del fornitore, delle "istruzioni per l'uso" del sistema di IA *ex* art. 13 e nelle forme di cooperazione quale, ad esempio, quella instaurata *ex* art. 60, par. 4, lett. h)

[91] J. SCHUETT, *Risk management in the artificial intelligence act*, in *European Journal of Risk Regulation*, 2023, p. 1.

nell'ambito delle cd. «prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA».

Ai sensi dell'art. 35 GDPR, il titolare del trattamento deve effettuare la DPIA quando un trattamento, in particolare se basato su nuove tecnologie, può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, tenuto conto della sua natura, portata, contesto e finalità. Tale obbligo ricorre, in particolare, oltre alle ipotesi stabilite dalle autorità di controllo (par. 4), nei casi di trattamenti automatizzati che producono effetti giuridici o incidono significativamente sugli interessati, di trattamenti su larga scala di categorie particolari di dati o di dati relativi a condanne penali e reati, nonché di sorveglianza sistematica su larga scala di spazi accessibili al pubblico (par. 3).

Le analogie fra i suddetti tre strumenti di gestione del rischio sono evidenti.

In primo luogo, sia il RMS e la FRIA che la DPIA si configurano come meccanismi di prevenzione, atti a individuare e mitigare i rischi rispettivamente prima che il sistema di IA ad alto rischio sia messo in servizio e utilizzato o il trattamento dei dati a "rischio elevato" abbia inizio. In tal modo, essi condividono lo scopo di orientare verso soluzioni rispettose dei diritti fondamentali fin dalla loro progettazione, secondo i principi di compliance *by design* e *by default*[92].

Un ulteriore elemento comune consiste nella natura iterativa dei tre strumenti. RMS, FRIA e DPIA, rispettivamente agli artt. 9, par. 2, e 27, par. 2, *AI Act* e dall'art. 35, par. 11, GDPR, non stabiliscono adempimenti *una tantum*, quanto piuttosto processi dinamici di valutazione e aggiornamento continuo, in grado di cogliere il carattere mutevole della realtà di impiego.

Infine, sia la FRIA che la DPIA possono essere applicate a più sistemi di IA o trattamenti che presentino caratteristiche analoghe. L'art. 27, par. 2, *AI Act* consente infatti al *deployer* di «fare affidamento su valutazioni d'impatto sui diritti fondamentali precedentemente condotte o su valutazioni d'impatto esistenti effettuate dal fornitore», riducendo la duplicazione degli adempimenti. Un principio affine è riconosciuto anche nel GDPR dove una singola DPIA può riguardare una serie di trattamenti simili che presentano rischi analoghi (considerando 92), ed è ammessa la

[92] M. ALMADA, J. MARANHÃO, G. SARTOR, *Article 25. Data Protection by Design and by Default*, in I.S.G. DÖHMANN ET AL. (a cura di), *General data protection regulation: article-by-article commentary*, New York, 2023, p. 580.

possibilità di riutilizzare valutazioni d'impatto già condotte quando il trattamento trova fondamento in una norma dell'Unione o di uno Stato membro (art. 35, par. 10)[93].

Sono tali analogie che, peraltro, hanno spinto il legislatore dell'UE a prevedere forme di un loro coordinamento. L'art. 27, par. 5, *AI Act* stabilisce infatti che, qualora gli obblighi derivanti dalla FRIA risultino già adempiuti attraverso una precedente DPIA, la prima si limita a "completare" quest'ultima, favorendo sinergie tra i due strumenti[94].

4. Conclusioni

L'analisi svolta suggerisce alcune considerazioni conclusive circa la portata dell'*AI Act* e l'influenza su di esso esercitata dalla normativa europea preesistente, in particolare dal *New Legislative Framework* e dal GDPR, per quanto riguarda soprattutto l'approccio basato sul rischio.

La contaminazione tra i diversi modelli normativi reca con sé alcuni indiscutibili benefici e vantaggi.

Innanzitutto, il Regolamento sull'IA sfrutta i punti di forza di un'esperienza normativa, il NFL, che ha già dato prova di una buona riuscita nelle fasi di sviluppo degli standard tecnici, ed in quelle di certificazione e vigilanza di classi di prodotti tra loro differenti e a rischio elevato[95].

Allo stesso modo, il riferimento a istituti e strumenti tipici della disciplina sulla protezione dei dati personali, quali la profilazione, la

---

[93] Cfr. EDPB, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, 20 ottobre 2020.

[94] Nonostante tali convergenze, permangono significative differenze di oggetto e di funzione. La DPIA è circoscritta al trattamento dei dati personali e si concentra sulla protezione della privacy e delle libertà correlate, mentre la FRIA presenta un ambito più ampio, esteso all'intero spettro dei diritti fondamentali garantiti dalla Carta dei diritti fondamentali dell'Unione europea, tra cui la dignità umana, la non discriminazione, la libertà di espressione e la tutela dei dati personali. Inoltre, rispetto alla DPIA, la FRIA comporta oneri procedurali più elevati. Infatti, la FRIA prevede che i suoi risultati debbano essere comunicati all'autorità di vigilanza del mercato *ex* art. 27, par. 3, con la sola eccezione dei casi di cd. deroga alla procedura di valutazione della conformità di cui all'art. 46, par. 1. Per la DPIA, invece, il titolare è tenuto a consultare preventivamente l'autorità di controllo solo nel caso in cui la valutazione d'impatto evidenzi rischi elevati che non possono essere mitigati con misure tecniche e organizzative adeguate (considerando 84 GDPR). A. THOMAIDOU, K. LIMNIOTIS, *Navigating Through Human Rights in AI: Exploring the Interplay Between GDPR and Fundamental Rights Impact Assessment*, in *Journal of Cybersecurity and Privacy*, 2025, p. 1; A. MANTELERO, *The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template*, cit., p. 3.

[95] M. ALMADA, N. PETIT, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, cit., p. 21.

biometria, la trasparenza, e la gestione del rischio fornisce al regolamento in analisi un repertorio di soluzioni giuridiche già consolidate anche a livello giurisprudenziale, sia ad opera della Corte di giustizia dell'UE, sia delle Corti e autorità garanti della privacy nazionali, che in più paesi membri sono dotate di competenze per l'*enforcement* dell'*AI Act*[96].

Tuttavia, l'ampiezza e a volte genericità dei riferimenti normativi presenti nell'*AI Act*, lo espone ad alcuni rilievi critici, volti a evidenziare un disallineamento sistematico tra i fini perseguiti, e quindi la protezione dei diritti fondamentali, e gli strumenti prescelti per conseguirli, derivati prevalentemente dal diritto della sicurezza dei prodotti[97].

Sul piano formale, in primo luogo, i diritti fondamentali, pur ampiamente richiamati nei considerando, trovano un riscontro più limitato nelle singole disposizioni ove compaiono solo in forma ancillare rispetto alla salute e alla sicurezza (ad esempio, artt. 5, 9, par. 2, e 14, par. 2).

Inoltre, sebbene sia la sicurezza dei prodotti sia la tutela dei diritti fondamentali perseguano, in ultima analisi, la prevenzione e la mitigazione dei rischi[98], esse, tuttavia, impiegano due approcci divergenti per raggiungere tali obiettivi. A tal proposito, il modello NLF, fatto proprio dall'*AI Act*, si fonda su procedure standardizzate di valutazione e gestione del rischio – tramite parametri tecnici, prove di conformità e test di sicurezza – finalizzati a contenerlo entro soglie considerate "accettabili" *ex ante* dal legislatore.

Viceversa, le normative sulla tutela dei diritti fondamentali si basano sui principi di proporzionalità e sul bilanciamento tra diritti e interessi potenzialmente confliggenti, richiedendo così un'analisi caso per caso con l'obiettivo di perseguire un livello di protezione quanto più elevato

---

[96] EDPB, *Dichiarazione 3/2024 sul ruolo delle autorità di protezione dei dati nel quadro del regolamento sull'intelligenza artificiale*, 16 luglio 2024.

[97] I. KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, in *Journal of risk research*, 2024, p. 1; E. CIRONE, *L'*AI Act *e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in *Quaderni AISDUE - Fascicolo speciale n. 2/2024*, p. 1; O. POLLICINO, G. DE GREGORIO, F. BAVETTA, F. PAOLUCCI, *Regolamento AI, la "terza via" europea lascia troppi nodi irrisolti: ecco quali*, *Agenda Digitale*, 21 maggio 2021; M. VEALE, F.Z. BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act - Analysing the good, the bad, and the unclear elements of the proposed approach*", in *Computer Law Review International*, 2021, p. 97; M. ALMADA, N. PETIT, *The EU AI Act: A Medley of Product Safety and Fundamental Rights?*, cit., p. 13.

[98] M. ALMADA, N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, cit., p. 105, ove si richiama a dimostrazione di ciò l'art. 38 della Carta dei diritti fondamentali, in materia di protezione del consumatore.

possibile, volto all'eliminazione di qualsiasi tipo di rischio a prescindere dal fatto che possa considerarsi accettabile o meno.

Tale impostazione distonica dell'*AI Act* secondo cui l'obiettivo della tutela dei diritti fondamentali è perseguito attraverso il modello NFL, da un lato, consegue alla scelta del legislatore europeo di assumere ad oggetto della regolazione il sistema di IA in quanto prodotto e non, invece, quale fonte di attribuzione diretta di diritti fondamentali, come avviene invece nel GDPR per il "trattamento dei dati personali" nei confronti dei diritti dell'interessato *ex* artt. 12-17 e 20[99]. Dall'altro lato, fa sì che il concetto di rischio come declinato nell'*AI Act*, ed in linea con il NFL, risulti intrinsecamente collegato all'emersione di un danno. Nell'*AI Act*, infatti, il danno è misura della probabilità e gravità del rischio, a differenza di quanto previsto da strumenti di tutela dei diritti fondamentali, quali il GDPR, rispetto al quale, come sostenuto dalla Corte di giustizia, «la semplice violazione degli obblighi di trattamento può costituire una lesione del diritto alla protezione dei dati personali, indipendentemente dall'esistenza di un danno materiale»[100].

Sul piano applicativo, la classificazione dei sistemi in quattro categorie di rischio, sebbene coerente con il principio di proporzionalità che permea l'intero impianto normativo, presenta un elevato grado di astrazione che si traduce in margini di incertezza non marginali sul corretto inquadramento di un sistema all'interno della corrispondente categoria di rischio. Ciò fa sì che i sistemi di intelligenza artificiale possano essere collocati in classi di rischio non adeguate, sottostimando o sovrastimando il loro livello di pericolosità, con conseguenze rilevanti in termini tanto di effettività nella tutela dei diritti fondamentali quanto della soggezione degli operatori economici a oneri eccessivi che incidono negativamente sulla loro capacità d'innovazione[101].

---

[99] Tale scelta è stata oggetto di rilievo da parte da un gruppo di associazioni civili, cfr. EDRI ET ALL, *An EU Artificial Intelligence Act for Fundamental Rights - A Civil Society Statement*, 2021, par. 5.

[100] Corte giust., 25 gennaio 2024, causa C-687/21, *BL v. MediaMarktSaturn Hagen-Iserlohn GmbH*, ECLI:EU:C:2024:72, parr. 56-61; Corte giust., 4 maggio 2023, causa C-300/21, *Österreichische Post AG*, ECLI:EU:C:2023:370, parr. 33-42. V. P. PAŁKA, *Data Management Law for the 2020s: The Lost Origins and the New Needs*, in *Buffalo Law Review*, 2020, p. 559.

[101] M. EBERS, *Truly Risk-based Regulation of Artificial Intelligence How to Implement the EU's AI Act*, cit., p. 691; M. ALMADA, N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, cit., p. 95; D. LEUFER, F. HIDVEGI, A. ZORNETTA, *The Pitfalls of the European Union's Risk-Based Approach to*

Peraltro, occorre sottolineare che la classificazione *ex ante* dei sistemi di IA nei diversi livelli di rischio, fondata su parametri tassativi piuttosto che ispirata a clausole generali, costituisce un elemento di rigidità nell'applicazione del regolamento tale da imporre, verosimilmente, frequenti interventi di adeguamento della disciplina prevista alle continue e rilevanti evoluzioni tecnologiche[102]. Sebbene tale esigenza di aggiornamento sia stata contemplata dallo stesso *AI Act*, ai sensi degli artt. 7 e 97, la procedura all'uopo prevista interessa unicamente la modifica dell'Allegato III relativo ai sistemi ad alto rischio ed è sottoposta al ricorrere di condizioni cumulative stringenti[103]. Rimangono, quindi, esclusi da tale procedura di aggiornamento i sistemi a rischio inaccettabile, quelli ad alto rischio di cui all'allegato I e le rimanenti categorie di sistemi a rischio limitato o nullo[104].

Ciononostante, l'approccio basato sul rischio rappresenta l'innovazione più rilevante dell'*AI Act*, in quanto si pone al crocevia del rapporto tra tecnologia, mercato e diritti fondamentali. È una concezione del rischio che cessa di essere un concetto meramente quantitativo risultando invece un parametro giuridico sostanziale per valutare l'impatto delle tecnologie sui diritti fondamentali e sui valori fondativi dell'ordinamento europeo, con una connotazione quindi anche qualitativa.

Digital Rulemaking, cit., p. 162; M. VEALE, F. ZUIDERVEEN BORGESIUS, *Demystifying the Draft EU Artificial Intelligence Act-Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach*, cit., p. 105.

[102] M. CARTA, *Il Regolamento UE sull'Intelligenza Artificiale: alcune questioni aperte*, cit., p. 193 ss.

[103] L'art. 7, par. 1, *AI Act* prevede che: «a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III; b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.» La problematica sembra essere particolarmente rilevante considerato che, secondo la Commissione europea, in questa classe ricadrebbero tra il 5-15% della totalità dei sistemi, cfr. European Commission, *Impact Assessment Accompanying the Proposal for Artificial Intelligence Act*, cit., par. 6.1.3.

[104] La rigidità del modello di classificazione dei sistemi di IA può essere in parte attenuata dal rinvio alle norme tecniche armonizzate. Così, ad esempio, l'art. 15, par. 1, *AI Act* stabilisce che i sistemi di IA ad alto rischio debbano garantire livelli adeguati di accuratezza, robustezza e sicurezza informatica, senza tuttavia precisarne la soglia. La determinazione di ciò che costituisce un livello "adeguato" è rimessa ai fornitori, che possono conformarsi alle pertinenti norme tecniche armonizzate o ad altri standard di riferimento. Benché anche tali norme siano soggette al rischio di obsolescenza per effetto dell'evoluzione tecnologica, la loro revisione risulta procedimentalmente più agevole rispetto alla modifica di un atto legislativo, mitigando così, almeno in parte, la problematica in questione, cfr. M. ALMADA, N. PETIT, *The EU AI Act: Between the rock of product safety and the hard place of fundamental rights*, cit., p. 100.

In questa prospettiva, l'*AI Act* si propone l'obiettivo ambizioso, ancora al di là dall'essere realizzato, di coniugare la regolamentazione delle dinamiche economiche alla base del funzionamento del mercato con la dimensione assiologica della tutela dei diritti fondamentali. La sfida da affrontare richiede che questi due aspetti, nella strategia digitale dell'Unione, non siano considerarti separatamente consentendo invece l'ingresso e l'applicazione dei principi e dei diritti contenuti nella Carta dei diritti fondamentali a quei settori più tecnologicamente avanzati e innovativi della società digitale europea.

Nel caso specifico la riuscita di tale operazione sembra essere legata, tra l'altro, al dialogo tra il CEN-CENELEC e la Commissione europea, al fine di consentire la trasposizione della tutela dei diritti fondamentali all'interno di standard di tipo tecnico, in modo tale da tradurre l'approccio basato sul rischio in un modello di *accountability* sostanziale dove la protezione di tali diritti può rappresentare un vincolo non meramente formale, ma un parametro sostanziale di legittimità e sostenibilità dell'innovazione tecnologica[105].

[105] Una volta realizzato tale obiettivo, l'*AI Act* potrà dispiegare i propri effetti extra-UE e, di conseguenza, l'Unione potrà affermare la propria sovranità tecnologica, fondata sulla centralità della dignità e della libertà della persona. Sulla capacità dell'*AI Act* di imporsi quale standard globale, in senso positivo, v. N.A. SMUHA, *From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence*, in *Law, Innovation and Technology*, 1/2021, p. 58. In senso negativo, U. PAGALLO, *Why the AI Act Won't Trigger a Brussels Effect*, in *AI Approaches to the Complexity of Legal Systems* (Springer 2024), Forthcoming, disponibile online all'indirizzo https://ssrn.com/abstract=4696148. Per una ricostruzione critica sul tema v. B. CRUM, *Brussels effect or experimentalism? The EU AI Act and global standard-setting*, in *Internet Policy Review*, 3/2025, p. 14.

Il *Digital Market Act*, un nuovo paradigma per la politica di concorrenza dell'UE nei mercati digitali: tra regolamentazione e diritto antitrust

di FRANCESCO ROSSI DAL POZZO* e MARCO GUIDI**

SOMMARIO: 1. Introduzione. – 2. L'interazione tra il diritto della concorrenza e la regolamentazione economica. – 2.1. Profili distintivi…. – 2.2. …e di sovrapposizione. – 2.3. L'interazione tra diritto della concorrenza e regolamentazione economica nel diritto dell'UE. – 3. La natura ibrida del *Digital Market Act*. – 3.1. Indici che riconducono il *Digital Market Act* alla regolamentazione economica. – 3.1.1. L'ambito di applicazione materiale del DMA. – 3.1.1.1. L'applicabilità del DMA ai mercati interessati da fallimenti di mercato. – 3.1.1.2. L'intervento asimmetrico nei confronti dei *gatekeeper*. – 3.1.2. L'art. 114 TFUE quale base giuridica del DMA. – 3.1.3. Gli obblighi *ex ante* del DMA. – 3.1.4. Transitorietà ed eccezioni di natura economica. – 4. Analogie tra il *Digital Market Act* e il diritto della concorrenza. – 4.1. Analogie sotto il profilo degli obiettivi. – 4.2. Analogie sotto il profilo della codificazione della prassi antitrust. – 5. Conclusioni.

1. Introduzione

L'accelerazione dei processi di digitalizzazione, favorita dalla pandemia di COVID-19, ha generato indiscussi benefici economici sia per i consumatori, sotto forma di disponibilità di un'ampia varietà di prodotti e servizi innovativi, sia per le imprese, che possono sfruttare le opportunità dispiegate dal commercio elettronico e da un mercato globale sempre più interconnesso. Tale evoluzione, seppur non sia confinata ad un settore specifico, costituendo «il fondamento medesimo di tutti i sistemi economici innovativi moderni», è stata colta, in particolare, dalle cd. piattaforme *online*, ossia le imprese che più si sono «dimostrate foriere di innovazione nell'economia digitale», grazie alla propria attività di

* Professore ordinario di diritto dell'Unione europea presso l'Università degli Studi di Milano, Dipartimento di Diritto pubblico, italiano e sovranazionale.

** Ricercatore TDA di diritto dell'Unione europea presso l'Università degli Studi di Roma UnitelmaSapienza, Dipartimento di Diritto e Società Digitale.

Sebbene il presente contributo sia frutto di riflessioni comuni e condivise, Francesco Rossi Dal Pozzo è autore dei §§ 1, 2, 2.1, 2.2 e 2.3, Marco Guidi è autore dei §§ 3, 3.1, 3.1.1, 3.1.1.1, 3.1.1.2, 3.1.2, 3.1.3, 3.1.4, 4, 4.1 e 4.2. Il § 5 è, invece, da imputarsi ad entrambi gli autori.

intermediazione *online* di utenti commerciali e finali, fondata sull'uso di tecnologie digitali, quali dati e algoritmi[1].

Tali piattaforme *online* rappresentano mercati innovativi che, caratterizzati da elevate barriere all'ingresso, ridotta contendibilità e concentrazione del potere economico[2], hanno contribuito a mutare le dinamiche concorrenziali e hanno posto sfide inedite al diritto della concorrenza dell'Unione europea. La repentina affermazione di questi operatori economici quali monopolisti o oligopolisti dei rispettivi mercati

[1] Commissione europea, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 def. V. B. NASCIMBENE, *Il mercato unico digitale è una nuova frontiera dell'integrazione europea?*, in *questa Rivista*, 2025, p. 105.

[2] Sul processo di revisione della politica antitrust in conseguenza della rivoluzione digitale sono stati condotti numerosi studi da parte delle autorità garanti della concorrenza, tanto a livello nazionale: Swedish Competition Authority, *Competition in Digital Markets in Sweden*, 2021; French Competition Authority, *Contribution to the Debate on Competition Policy and Digital Challenges*, 2020; UK Competition and Markets Authority, *Online Platforms and Digital Advertising – Market Study Report*, 2020; U.S. House of Representatives, *Subcommittee on Antitrust, Commercial, and Administrative Law, Investigation of Competition in Digital Markets – Majority Staff Reports and Recommendations*, 2020; Austrian Competition Authority, '*Digitalisation and Competition Law'*, 2020; Australian Competition and Consumer Commission, *Digital Platforms Inquiry*, 2019; German Commission "Competition Law 4.0", *A New Competition Framework for the Digital Economy*, 2019; quanto a livello sovranazionale: Nordic Competition Authorities, *Digital Platforms and the Potential Changes to Competition Law at the European Level*, 2020; Belgian Competition Authority, Dutch Authority for Consumers & Markets, Luxembourg Conseil de la Concurrence, *Joint Memorandum on Challenges Faced by Competition Authorities in a Digital World*, 2019; Global Antitrust Institute, *Report on the Digital Economy*, 2020; G7 Competition Authorities, *Common Understanding on "Competition and the Digital Economy"*, 2019. Sul tema, in dottrina v. D.A. CRANE, *Antitrust after the coming wave*, in *New York University Law Review*, 4/2024, p. 1187; J. TIROLE, *Competition and the Industrial Challenge for the Digital Age*, in *Annual Review of Economics*, 15/2023, p. 573; E. FAZIO, *Adapting Competition Law to the Digital Transition. Two Challenges*, in *European Papers*, 3/2022, p. 981; E. CALVANO, M. POLO, *Market power, competition and innovation in digital markets: A survey*, in *Information Economics and Policy*, 2021, p. 54; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di Digital Market Act*, in *I Post di AISDUE*, 2/2021, p. 31; J. FURMAN ET AL., *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, Londra, 2019; J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era*, Lussemburgo, 2019; Chicago Booth George J. Stigler Center, *Report from the Committee for the Study of Digital Platforms*, 2019; N. PETIT, *Are 'Fangs' Monopolies? A Theory Of Competition Under Uncertainty*, Working paper, 2019; B. LUNDQVIST, *Regulating competition in the digital economy - With a special focus on platforms*, in B. LUNDQVIST, M. GAL (a cura di), *Competition Law for the Digital Economy*, Cheltenham, 2019; A. EZRACHI, *EU Competition Law Goals and the Digital Economy*, in *Oxford Legal Studies Research Paper*, 17/2018, p. 1; A. EZRACHI, M. STUCKE, *Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy*, Harvard, 2016; R.A. POSNER, *Antitrust in the New Economy*, in *Antitrust Law Journal*, 2001, p. 925.

digitali ha innescato un'intensa attività di *enforcement*, volta a verificare che tali posizioni di dominanza fossero state raggiunte e venissero mantenute legittimamente. Questa attività ha interessato i principali strumenti del diritto della concorrenza, ossia il divieto di intese restrittive *ex* art. 101, par. 1, TFUE[3] e di abuso di posizione dominante *ex* art. 102 TFUE[4], nonché il controllo delle concentrazioni, disciplinato dal Regolamento (CE) n. 139/2004[5].

Ciononostante, l'azione della Commissione europea e delle autorità nazionali garanti della concorrenza è stata bersaglio di critiche per la tardività degli interventi repressivi o, addirittura, per un certo *laissez faire*, che avrebbero minato la capacità dell'UE e degli Stati membri di garantire il corretto svolgimento delle dinamiche competitive dei mercati digitali, causando la formazione di posizioni di "superdominanza"[6].

Per far fronte a queste problematiche, la Commissione europea, nella comunicazione *Una politica della concorrenza pronta a nuove sfide*[7], ha formulato due approcci che, sebbene distinti, sono integrati sinergicamente.

Il primo, relativo alla necessità di attuare una «revisione inedita per

---

[3] P. MANZINI, *Diritto antitrust dell'Unione europea*, Torino, 2022, p. 39; M. D'OSTUNI, *Il concetto d'intesa*, in L.F. PACE (a cura di), *Dizionario sistematico del diritto della concorrenza*, 2020, Milano, p. 85

[4] V. F. FERRARO, *L'abuso di posizione dominante*, in B. CORTESE, F. FERRARO, P. MANZINI (a cura di), *Il diritto antitrust dell'Unione europea*, Torino, 2014, p. 45; P. FATTORI, M. TODINO, *La disciplina della concorrenza in Italia*, Bologna, 2010, p. 156; G. MONTI (a cura di), *EC Competition Law*, Cambridge, 2007, p. 159 ss.

[5] Regolamento (CE) n. 139/2004 del Consiglio, del 20 gennaio 2004, relativo al controllo delle concentrazioni tra imprese ("Regolamento comunitario sulle concentrazioni"), in *GUUE* L 24 del 29 gennaio 2004, p. 1. Per una disamina dei principali provvedimenti adottati dalle Autorità antitrust in ambito digitale si rimanda a OECD, *Handbook on Competition Policy in the Digital Age*, 2022; D. MANDRESCU (a cura di), *EU Competition Law and the Digital Economy: Protecting Free and Fair Competition in an Age of Technological (R)evolution*, The Hague, 2020. Per un approfodimento sulle operazioni di concentrazione nel medesimo ambito, v. OECD, *Theories of Harm for Digital Mergers*, OECD Roundtables on Competition Policy Papers, 2023; M. BOURREAU, A. DE STREEL, *Big Tech Acquisitions: Competition & Innovation Effects and EU Merger Control*, CERRE Report, 2020.

[6] Corte giust., 10 novembre 2021, causa T-612/17, *Google and Alphabet v Commission (Google Shopping)*, ECLI:EU:T:2021:763, punto 182. V. J. FURMAN ET AL., *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, cit., p. 14; J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era*, cit., p. 42; Chicago Booth George J. Stigler Center, *Report from the Committee for the Study of Digital Platforms*, cit., p. 79.

[7] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Una politica della concorrenza pronta a nuove sfide, COM(2021)713 def.

portata e ambizione degli strumenti della politica della concorrenza», si è prefissato lo scopo di garantire che tutti i suoi pilastri fossero in grado di perseguire efficacemente le finalità originarie, in un contesto trasformato profondamente, quale è quello digitale[8]. Possono leggersi in questa prospettiva la revisione del concetto di mercato rilevante[9], le nuove discipline sugli accordi orizzontali[10] e verticali[11], nonché la recente proposta di modifica al Regolamento n. 1/2003[12].

Tuttavia, sul presupposto che la politica della concorrenza non è sempre in grado di risolvere da sé tutti i problemi strutturali che caratterizzano i mercati digitali, la Commissione ha formulato un secondo approccio diretto all'adozione di una normativa *ad hoc*, indirizzata alle piattaforme *online* e compresa nel cd. pacchetto relativo alla legge sui servizi digitali[13]. Il progetto normativo in questione è stato adottato, nel

[8] *Idem*, p. 3.

[9] Comunicazione della Commissione sulla definizione del mercato rilevante ai fini dell'applicazione del diritto dell'Unione in materia di concorrenza, 8 febbraio 2024, COM(2023)6789 def.

[10] Comunicazione della Commissione Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale, 17 luglio 2023, COM(2023)4752 def.

[11] 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, in *GUUE* L 134 dell'11 maggio 2022, p. 4; Comunicazione della Commissione, Orientamenti sulle restrizioni verticali, 2022/C 248/01, in *GUUE* C248 del 30 giugno 2022, p. 1.

[12] European Commission, Commission Staff Working Paper, *Evaluation of Regulation 1/2003*, COM(2020) 740 def.

[13] A tal proposito, gli *Orientamenti politici per la prossima Commissione europea 2019-2024* hanno delineato sei politiche principali tra cui, per quanto qui interessa, quella relativa a «Un'Europa pronta per l'era digitale»; in tale contesto, la Commissione, con la comunicazione *Plasmare il futuro digitale dell'Europa* (COM(2020) 67), ha indicato tre obiettivi chiave, il cui scopo comune è quello di garantire che la transizione digitale sia guidata dai valori e dalla tutela dei diritti fondamentali su cui poggia il diritto dell'UE. Nella cornice del secondo obiettivo «Un'economia equa e competitiva», il 15 dicembre 2020, la Commissione europea ha presentato due proposte normative di regolamentazione delle piattaforme online. Dette proposte appaiono, per la verità, riduttive rispetto ai progetti concepiti in origine. Secondo l'intenzione iniziale, infatti, la Commissione mirava ad articolare una proposta normativa strutturata nel: (*i*) *Digital Services Package*, composto da due proposte di regolamento, ovvero la legge sui mercati digitali ("*Digital Market Act*") e la legge sui servizi digitali ("*Digital Service Act*"), v. European Commission, *Inception Impact Assessment - Digital Services Act Package: Ex ante regulatory instrument for large online platforms with significant network effects acting as gate-keepers in the European Union's internal market*, 2020; (*ii*) il cd. *New Competition Tool*, che avrebbe consentito di munire le autorità antitrust di uno strumento di azione rapida, maggiormente rispondente alle caratteristiche dei mercati digitali, v. European Commission, *Inception impact assessment - New Competition Tool*, 2020, sul

novembre 2022, dal legislatore dell'UE quale Regolamento (UE) 2022/1925 sull'equità e contendibilità dei mercati digitali, ossia il cd. *Digital Markets Act* ("DMA")[14].

Come si avrà modo di osservare, si tratta di un regolamento che, sebbene formalmente incardinato nella categoria della cd. regolamentazione economica, ossia quel *corpus* normativo volto a modificare le condotte degli operatori economici[15], presenta alcuni tratti distintivi del diritto della concorrenza, segnatamente della disciplina antitrust. Una forma di "ibridazione" normativa che rischia di condurre a

---

quale si rimanda a H. SCHWEITZER, *The New Competition Tool: Its institutional set up and procedural design - Expert Report*, Lussemburgo, 2021. Tuttavia, la valutazione d'impatto relativa a detto *New Competition Tool* e quella relativa alla proposta di legge sui mercati digitali sono state combinate in un unico atto che accompagna quest'ultima proposta legislativa. È stato quindi adottato il solo *Digital Services Package* comprensivo dei citati *Digital Market Act* e del *Digital Service Act*.

[14] Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in *GUUE* L 265 del 12 ottobre 2022, p. 1. Per una prima introduzione sul *Digital Makert Act* v. G. CARATOZZOLO, *The Digital Markets Act in action: analysis of the early practice of the Commission*, in *questa Rivista*, 3/2024, p. 141; F. SPORTA CAPUTI, *Il* Digital Market Act *(Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione* ex ante *dell'abuso di posizione dominante*, in *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito*, 1/2024, p. 64; E.A. RAFFAELLI, *I mercati digitali e le norme di regolazione: tra limiti del diritto antitrust e nuove modalità di intervento* ex ante, in *Rivisti di Diritto Industriale*, 2024, p. 45; M. OROFINO, Il Digital Market Act*: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust*, in S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO (a cura di), *La regolazione europea della società digitale*, Torino, 2024, p. 175; G. COLANGELO, *DMA, Begins*, in *Journal of Antitrust Enforcement*, 45(11), 2023, p. 110; A. IANNOTTI DELLA VALLE, *Il* Digital Markets Act *e il ruolo dell'Unione europea verso un costituzionalismo digitale*, in *Giurisprudenza Costituzionale*, 2022, p. 1868; G. COLANGELO, *The European Digital Markets Act and antitrust enforcement: a liaison dangereuse*, in *European Law Review*, 3/2022, p. 587; M. LIBERTINI, *Il regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Riv. trim. dir. pubbl.*, 4/2022, p. 1069; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, in *I Post di AISDUE*, 2/2021; L. CABRAL ET AL., *The EU Digital Markets Act. A Report from a Panel of Economic Experts*, Joint Research Centre Report - Publications Office of the European Union, Lussemburgo, 2021; M. CAPPAI, G. COLANGELO, *Taming digital gatekeepers: the 'more regulatory' approach to antitrust law*, in *Computer Law & Security Review*, 41/2021, p. 1; A. DE STREEL, *Digital Markets Act: Making economic regulation of platforms fit for the digital age*, CERRE Report, 2020. Sul processo di adozione del DMA v. P. IBAÑEZ COLOMO, *The Draft Digital Markets Act: A Legal and Institutional Analysis*, in *Journal of European Competition Law & Practice*, 2021, p. 561; M. BOTTA, *Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila*, in *Journal of European Competition Law & Practice*, 7/2021, p. 500.

[15] R.S. KHEMANI, D. M. SHAPIRO, *Glossary of Industrial Organisation Economics and Competition Law*, OECD, 1993.

tensioni sul piano applicativo.

2. L'interazione tra il diritto della concorrenza e la regolamentazione economica

2.1. Profili distintivi…

La natura ibrida del DMA ha rivitalizzato il dibattito sul rapporto tra regolamentazione e diritto della concorrenza, emerso nell'ambito delle politiche comunitarie di armonizzazione e liberalizzazione settoriale, dirette alla realizzazione del Mercato unico[16].

Tali categorie normative presentano elementi distintivi che ne agevolano il rispettivo inquadramento sistematico[17].

Innanzitutto, il diritto della concorrenza fornisce un quadro generale entro cui gli attori di mercato sono liberi di perseguire autonomamente i propri obiettivi economici, limitati – in negativo e in maniera decentrata – da una serie di divieti rispetto a condotte, quali le intese restrittive della

[16] Per una prima introduzione sul rapporto tra regolamentazione economica e diritto della concorrenza v. OECD, *Competition Enforcement and Regulatory Alternatives*, OECD Competition Committee Discussion Paper, 2021; OECD, *The Regulated Conduct Defence - Series Roundtables on Competition Policy N° 116*, 2011, DAF/COMP(2011)3; N. DUNNE (a cura di), *Competition Law and Economic Regulation: Making and Managing Markets*, Cambridge, 2015; L. PROSPERETTI, *I rapporti tra regolazione e tutela della concorrenza. Teoria economica e esperienze recenti,* in *Mercato conc. reg.*, 2002, p. 277 ss.; S. CASSESE, *Regolazione e concorrenza*, in G. TESAURO, M. D'ALBERTI (a cura di), *Regolazione e Concorrenza*, Bologna, 2000, p. 11 ss. Con specifico riferimento al settore digitale, v. G. MUSCOLO, *Il rapporto tra applicazione/regolamentazione antitrust e il DMA*, in J. MOSCIANESE, O. POLLICINO (a cura di), *Concorrenza e regolamentazione nei mercati digitali. Lo stato dell'arte dopo l'entrata in vigore del* Digital Markets Act, Torino, 2024, p. 99; N.M. BELLOSO, N. PETIT, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, in *European Law Review*, 2023, p. 391; M.V. LA ROSA, *Lo scopo della regolamentazione*, in L. BOLOGNINI, E. PELINO, M. SCIALDONE (a cura di), Digital Service Act *e* Digital Market Act, Milano, 2023, p. 239; OECD, *Ex ante regulation of digital markets*, OECD Competition Committee Discussion Paper, 2021; A. DE STREEL, *Digital Markets Act: Making economic regulation of platforms fit for the digital age*, cit., p. 86; UK Competition and Markets Authority, *Regulation and Competition. A Review of the Evidence*, cit., parr. 1.3 - 2.4; German Commission "Competition Law 4.0", *A New Competition Framework for the Digital Economy*, cit., p. 49; J. DREXL, F. DI PORTO (a cura di), *Competition law as regulation*, Cheltenham, 2015; M. CAPPAI, G. COLANGELO, *Taming digital gatekeepers: the 'more regulatory' approach to antitrust law*, cit., p. 5.

[17] M. CAPPAI, G. COLANGELO, *Taming digital gatekeepers: the 'more regulatory' approach to antitrust law*, cit., p. 3 ss.; C. OSTI, *Il* Digital Market *Act tra regolazione e concorrenza*, in G. CAGGIANO, G. CONTALDI, P. MANZINI (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2012, p. 123; OECD, *Ex ante regulation of digital markets*, cit., p. 12; OECD, *Competition Enforcement and Regulatory Alternatives*, cit., p. 6; G. MONTI, *Managing the Intersection of Utilities Regulation and EC Competition Law*, in *Competition Law Review*, 2/2008, p. 123.

concorrenza e l'abuso di posizione dominante, che rischiano di alterare l'*agere* competitivo delle imprese e, di conseguenza, diminuire il benessere del consumatore e l'innovazione.

La regolamentazione, invece, agisce in modo prescrittivo. Il comportamento delle imprese viene indirizzato – in positivo e in maniera accentrata – al perseguimento di determinate finalità di stampo economico-sociale, attraverso l'imposizione di divieti e di obblighi fondati sul bilanciamento, a monte, degli interessi in gioco. La libertà degli operatori economici è, dunque, delimitata fin da principio dal legislatore per conseguire finalità specifiche.

Questa distinzione è spesso descritta con la dicotomia "*ex post*" ed "*ex ante*" che descrive, rispettivamente, l'intervento a posteriori del diritto antitrust diretto a sanzionare le distorsioni già verificatesi, in base alla valutazione sulla sussistenza, o meno, di una violazione alle prescrizioni previste, in opposizione all'obbligo di conformità a priori rispetto ai requisiti modellati dalla regolamentazione[18].

Ancora, mentre il diritto della concorrenza ha un ambito applicativo trasversale all'intero Mercato unico, la regolamentazione economica ha matrice settoriale e si attua, infatti, per il tramite di autorità *ad hoc*, dotate delle competenze tecniche e dei poteri necessari ad operare nel contesto di riferimento.

Un'ulteriore linea di distinzione riguarda la diversa stabilità nel tempo delle due categorie normative. Il diritto della concorrenza ha una vocazione strutturalmente permanente, poiché presidia in modo continuo il corretto funzionamento del mercato attraverso regole generali che non dipendono dalle caratteristiche contingenti di un determinato settore. La regolamentazione economica presenta, invece, un carattere transitorio, in quanto è concepita per avere effetto fintantoché permangono specifiche condizioni che impediscono o alterano il naturale dispiegamento delle dinamiche concorrenziali.

Infine, dal punto di vista formale, la distinzione tra diritto della concorrenza e regolamentazione riguarda la loro formulazione normativa. Il diritto antitrust si fonda su disposizioni ampie, articolate in clausole generali quali "mercato rilevante", "posizione dominante" e "abuso" ai sensi dell'art. 102 TFUE che richiedono un'interpretazione caso per caso. La regolamentazione, viceversa, si attua attraverso un articolato normativo

[18] Sfugge a siffatto inquadramento il controllo sulle operazioni di concentrazione, che si svolge anteriormente rispetto alla realizzazione dell'operazione stessa.

di obblighi dettagliati, come quelli in materia di non discriminazione, trasparenza, determinazione dei prezzi, accesso equo a infrastrutture essenziali o servizi indispensabili, nonché tutela dei consumatori[19].

2.2. …e di sovrapposizione

Nonostante queste caratteristiche distintive, la relazione tra diritto della concorrenza e regolamentazione economica resta difficile da tracciare con nettezza.

Ciò è dovuto al fatto che entrambe le discipline mirano a rimediare ai cd. fallimenti di mercato, ossia condizioni che, non consentendo ad un determinato mercato di raggiungere un equilibrio soddisfacente dal punto di vista economico, giustificano l'intervento pubblico nella duplice veste di diritto della concorrenza e di regolamentazione economica[20]**.**

Nello specifico, il diritto della concorrenza è concepito per intervenire rispetto ad una specifica categoria di fallimento, ossia il "potere di mercato**",** che è contrastato non in quanto tale, ma solo qualora acquisito, mantenuto o esercitato attraverso comportamenti abusivi o collusivi vietati.

Diversamente, la regolamentazione economica non si limita a intervenire sul solo potere di mercato, ma è concepita per correggere altre tipologie di fallimento che spesso ne sono all'origine o ne costituiscono un corollario, quali esternalità, barriere all'ingresso, prezzi eccessivi, asimmetria informativa, immobilità dei fattori produttivi, *free riding* o, ancora, regimi monopolistici legali.

Questa area di parziale sovrapposizione tra le due discipline contribuisce a sfumarne i rispettivi confini applicativi e fa sì che esse possano essere concepite ora in modo alternativo, ora in modo complementare.

---

[19] Questa dicotomia conosce alcune eccezioni tanto sotto il profilo sostanziale, posto che anche il diritto della concorrenza, attraverso atti di *soft law* (linee guida, orientamenti, ecc.), norme *ad hoc* (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, in *GUUE* L 134 dell'11 maggio 2022, p. 4), prassi applicativa e interventi giurisprudenziali, stabilisce previsioni dettagliate *ex ante*, a cui gli operatori del mercato si conformano per limitare il rischio di incorrere nelle relative sanzioni; quanto sotto il profilo procedurale, poiché i poteri attribuiti alla Commissione europea dal regolamento 1/2003 nell'ambito degli impegni e dei rimedi strutturali possono conseguire obblighi dettagliati. V. C. OSTI, *Il* Digital Market *Act tra regolazione e concorrenza*, cit., p. 124 ss.

[20] OECD, *Independent Sector Regulators – Background Note Working Party No. 2 on Competition and Regulation,* 2019, DAF/COMP/WP2(2019)3, p. 7.

In particolare, il primo orientamento, consolidatosi nell'ordinamento giuridico statunitense, concepisce l'intervento regolatorio come sostitutivo a quello antitrust, in quanto non si limita a correggere le disfunzioni del mercato, ma mira a rimpiazzare del tutto gli esiti della dinamica concorrenziale[21]. In questo ambito, l'adozione della regolamentazione economica equivale a una scelta pubblica di sottrarre un determinato settore al funzionamento spontaneo delle forze di mercato, con conseguente compressione dello spazio di applicazione del diritto antitrust. Tale configurazione si riscontra, ad esempio, nei settori dell'energia, dei trasporti e delle professioni regolamentate, in cui la regolamentazione stabilisce standard tecnici, condizioni di utilizzo dell'infrastruttura di base e livelli tariffari al punto da non lasciare alcuno spazio residuale all'applicazione delle norme antitrust[22].

Di contro, il secondo orientamento considera l'efficienza dei mercati quale risultato dell'azione congiunta di entrambe le normative. La complementarità, in particolare, può operare in entrambe le direzioni, posto che, da un lato, l'*enforcement* antitrust è in grado di colmare le lacune della disciplina settoriale, reprimendo comportamenti elusivi o opportunistici che la regolazione non è in grado di prevenire e, dall'altro lato, la regolazione economica può rafforzare l'efficacia del primo predisponendo condizioni strutturali che agevolano l'ingresso di nuove imprese, aumentano la trasparenza del mercato e ostacolano il consolidamento ingiustificato del potere di mercato.

2.3. L'interazione tra diritto della concorrenza e regolamentazione economica nel diritto dell'UE

Il diritto dell'UE ha fatto proprio quest'ultimo orientamento. Esemplificativo, in tal senso, è il processo di liberalizzazione del settore

---

[21] La Corte Suprema degli Stati Uniti ha precisato in più occasioni che, quando il legislatore ha predisposto un apparato regolatorio specificamente volto a prevenire e rimediare ai danni alla concorrenza, il valore aggiunto derivante dall'applicazione parallela del diritto antitrust tende fisiologicamente a ridursi. In tali circostanze, si presume che i costi sistemici dell'*enforcement* antitrust – in termini di incertezza per gli operatori, rischio di interferenze con la regolazione e possibilità di sovra-deterrenza – possano risultare superiori rispetto ai benefici concorrenziali attesi, v. *Pacific Bell Telephone Co., d/b/a AT&T California et al. v Linkline Communications Inc* 555 US 438 (2009); *Verizon Communications, Inc. v. Law Offices of Curtis V. Trinko*, LLP, 540 US 398 (2003). Per un approfondimento si rimanda a D.W. CARLTON, R.C. PICKER, *Antitrust and Regulation*, in N.L. ROSE (a cura di), *Economic Regulation and its Reform*, Chicago, 2014, p. 25.

[22] OECD, *Competition Enforcement and Regulatory Alternatives*, cit., p. 7.

delle comunicazioni elettroniche, in cui all'applicazione del diritto antitrust si è affiancato il processo di revisione del quadro normativo settoriale[23]. In tale contesto, per quanto qui interessa, la Commissione europea ha descritto l'interazione tra il diritto della concorrenza e la regolamentazione economica come «un insieme coerente di misure atte a garantire un ambiente liberalizzato e concorrenziale»[24]. Secondo la Commissione, infatti, «[l]a combinazione di legislazione settoriale e applicazione delle regole della concorrenza ha dato buoni frutti», facilitando «l'accesso al mercato laddove gli operatori storici continuano a detenere forti posizioni e a controllare l'accesso alla maggioranza degli abbonati», e assicurando «che i nuovi operatori possano competere in modo effettivo»[25].

Si tratta di un rapporto al tempo stesso dinamico e strutturalmente integrato. Sul primo versante, la Commissione, nel riesame del quadro normativo del 1999, ha precisato che «se si fa maggiormente capo alle regole di concorrenza generali del Trattato diventa possibile sostituire gran parte della regolamentazione settoriale man mano che la concorrenza diventa effettiva», delineando un modello in cui la regolazione è destinata a ritirarsi dinnanzi al ripristino del gradiente competitivo del mercato[26]. Sul secondo versante, l'interazione tra le due discipline dà luogo a una circolarità virtuosa, poiché, da un lato, gli «atti comunitari adottati nel settore delle telecomunicazioni vanno interpretati in conformità delle norme di concorrenza, al fine di assicurare la migliore realizzazione possibile di tutti gli aspetti della politica comunitaria delle telecomunicazioni» e, dall'altro, «numerosi principi contenuti nel diritto sulla concorrenza […] sono inglobati in norme specifiche» del quadro regolatorio, con la conseguenza che «la Commissione […] nel compiere una valutazione in virtù delle regole di concorrenza, cercherà di basarsi per

[23] V. A. MANGANELLI, *Il principio di concorrenza fra antitrust e regolazione. il caso delle comunicazioni elettroniche,* in *Concorrenza e Mercato*, 2013, p. 279; M. CLARICH, G.F. CARTEI (a cura di), *Il codice delle comunicazioni elettroniche*, Milano, 2004; A. TIZZANO, *L'azione comunitaria nelle telecomunicazioni: interventi recenti e prospettive future*, in *Il diritto dell'informazione e dell'informatica*, 6/1998, p. 917;

[24] Comunicazione della Commissione sull'applicazione delle regole di concorrenza agli accordi in materia di accesso nel settore delle telecomunicazioni, in *GUCE* C 265/2, par. 149.

[25] Comunicazione della Commissione, Verso un nuovo quadro per l'infrastruttura delle comunicazioni elettroniche e i servizi correlati - Esame del 1999 del quadro normativo delle comunicazioni, COM(1999) 539 def., rispettivamente pp. 4 e 52.

[26] *Idem*, p. 6.

quanto possibile sui principi sanciti dalla legislazione in materia di armonizzazione»[27].

La formalizzazione di questo rapporto è intervenuta con la Raccomandazione del 2007 che identifica tre criteri cumulativi per stabilire quando i mercati rilevanti di prodotti e servizi del settore delle comunicazioni elettroniche possano essere oggetto di regolazione *ex ante*, ossia: (*i*) «la presenza di forti ostacoli non transitori all'accesso, che possono essere di carattere strutturale, giuridico o normativo»; (*ii*) «la struttura [del mercato] non tenda a produrre condizioni di concorrenza effettiva nell'arco di tempo considerato»; infine, (*iii*) «l'applicazione del diritto della concorrenza non sarebbe di per sé sufficiente a rimediare ai fallimenti di mercato esistenti»[28].

Questo approccio è stato successivamente consolidato dal legislatore dell'Unione con la Direttiva (UE) 2018/1972, che ha istituito il Codice europeo delle comunicazioni elettroniche[29]. Il Codice ha formalizzato un sistema di regolamentazione asimmetrica fondato sull'individuazione dei fornitori dotati di significativo potere di mercato su uno specifico mercato rilevante, riprendendo a tal scopo categorie e metodologie tipiche del diritto antitrust. Tale regime consente di imporre obblighi *ex ante* mirati alle sole imprese che, nel mercato rilevante, detengono una posizione dominante. Come esplicitato nella Direttiva, «in alcuni casi sussiste l'esigenza di dettare obblighi ex ante allo scopo di garantire lo sviluppo di

[27] Commissione europea, Comunicazione della Commissione sull'applicazione delle regole di concorrenza agli accordi in materia di accesso nel settore delle telecomunicazioni - quadro normativo, mercati rilevanti e principi (98/C 265/02), para. 57 e 58.

[28] Raccomandazione della Commissione del 17 dicembre 2007 relativa ai mercati rilevanti di prodotti e servizi del settore delle comunicazioni elettroniche che possono essere oggetto di una regolamentazione *ex ante* ai sensi della direttiva 2002/21/CE del Parlamento europeo e del Consiglio che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, in *GUCE* L 344 del 28 dicembre 2007, p. 65, considerando 5. Tali criteri sono stati ulteriormente sviluppati dalla Raccomandazione 2014/710 della Commissione, del 9 ottobre 2014, relativa ai mercati rilevanti di prodotti e servizi del settore delle comunicazioni elettroniche suscettibili di regolamentazione *ex ante*, in *GUUE* L 295/79, considerando 11. Per una ricostruzione del rapporto tra regolamentazione del settore delle comunicazioni elettroniche v. A. DE STREEL, *The relationship between competition law and sector specific regulation: The case of electronic communications*, in *Reflets et Perspectives de la Vie Economique*, 2008, p. 55.

[29] Direttiva 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il Codice europeo delle comunicazioni elettroniche, in *GUUE* 2018 L 321 del 17 dicembre 2018, p. 36.

un mercato concorrenziale», in modo da prevenire condotte escludenti e assicurare condizioni equamente contendibili[30].

In altri settori economici, l'*enforcement* antitrust ha operato come fattore propulsivo per l'intervento regolatorio. Ad esempio, nel mercato aeroportuale, la liberalizzazione dei servizi di *handling* e delle tariffe aeroportuali, non accompagnata da un adeguato presidio regolatorio, aveva agevolato una serie di pratiche discriminatorie oggetto di indagini antitrust nei primi anni '90[31]. Le criticità emerse in tali procedimenti – relative all'accesso ai servizi, alla trasparenza dei criteri tariffari e al trattamento differenziato tra vettori – hanno stimolato l'adozione della Direttiva 96/67/CE, relativa all'accesso al mercato dei servizi di assistenza a terra negli aeroporti della Comunità[32].

In linea teorica, la regolamentazione e il diritto della concorrenza possono trovarsi in tensione reciproca. Tuttavia, la giurisprudenza consolidata della Corte di giustizia dell'UE ha risolto tali conflitti nel senso che l'integrazione dei due regimi – e non la loro esclusione reciproca – sia funzionale al conseguimento degli obiettivi generali dell'Unione.

Nello specifico, la Corte di giustizia dell'Unione europea ha chiarito che la sussistenza di un quadro regolatorio settoriale non esclude, di per sé, l'applicazione delle norme antitrust. In particolare, nella sentenza *Deutsche Telekom*, la Corte ha precisato che, qualora la normativa settoriale si limiti a sollecitare o facilitare «l'adozione di comportamenti anticoncorrenziali autonomi da parte delle imprese» lasciando sussistere un margine, anche potenziale, di concorrenza suscettibile di essere ristretta o falsata dal comportamento dell'impresa dominante, quest'ultima può essere passibile dei profili di responsabilità *ex* art. 102 TFUE[33]. Di contro, la normativa antitrust non può trovare

---

[30] Considerando n. 161. Tali concetti sono stati ulteriormente precisati dalla Raccomandazione (UE) 2020/2245 della Commissione del 18 dicembre 2020 relativa ai mercati rilevanti di prodotti e servizi del settore delle comunicazioni elettroniche che possono essere oggetto di una regolamentazione *ex ante* ai sensi della direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche, in *GUUE* L 439/23 del 29 dicembre 2020.

[31] V. tra gli altri**,** Caso IV/34.801 - FAG - Flughafen Frankfurt/Main AG**;** Caso *V/35.613 - Alpha Flight Services/Aéroports de Paris*; Caso IV/M.616 - *Swissair / Sabena.*

[32] Direttiva 96/67/CE del Consiglio del 15 ottobre 1996 relativa all'accesso al mercato dei servizi di assistenza a terra negli aeroporti della Comunità, in *GUCE* L 272 del 25 ottobre 1996, p. 36. Sul rapporto tra prassi antitrust e regolamentazione nel settore aeroportuale v. OECD *Competition Policy and International Airport Services* DAFFE/CLP(98)3.

[33] Corte giust., 14 ottobre 2010, causa C-280/08 P, *Deutsche Telekom AG*, ECLI:EU:C:2010:603, punti 83 ss.

applicazione qualora un comportamento anticoncorrenziale venga imposto da un intervento regolatorio oppure quest'ultimo elimini ogni possibilità di comportamento concorrenziale, posto che, in tali circostanze, «la restrizione alla concorrenza non trova origine […] in comportamenti autonomi delle imprese»[34]. Come sottolineato dalla Corte nella sentenza *Telefónica*, le disposizioni in materia di concorrenza «sono di applicazione generale» e «non possono essere limitate dall'esistenza di un quadro normativo di regolazione *ex ante* adottato dal legislatore dell'Unione per specifici settori»[35].

Ciò non depone, tuttavia, per l'irrilevanza della regolamentazione nell'analisi concorrenziale. Al contrario, in settori fortemente regolati, come quello farmaceutico, la Corte ha evidenziato la necessità, per le autorità competenti, di considerare le specificità del quadro normativo, censurando pratiche di cd. *regulatory gaming* idonee, ad esempio, a ostacolare l'ingresso di nuovi operatori, quali le imprese di farmaci generici[36]. Nella causa *AstraZeneca*, la Corte ha affermato che un'impresa dominante non può utilizzare gli strumenti e le procedure regolatorie in modo da impedire o ritardare l'accesso al mercato di concorrenti[37]; mentre, nelle sentenze *F. Hoffmann-La Roche e Generics UK*, ha chiarito che la valutazione della concorrenza potenziale deve essere condotta tenendo

[34] *Idem*, punto 80. Sulla stessa scorta si pongono le sentenze della Corte giust., 17 febbraio 2011, causa C-52/09, *TeliaSonera*, ECLI:EU:C:2011:83, punti 49 e 50, e Corte giust., 9 settembre 2003, causa C-198/01, *Consorzio Industrie Fiammiferi*, ECLI:EU:C:2003:430, punti 53 ss. Sul tema v. OECD, *The Regulated Conduct Defence*, cit., p. 202 ss.

[35] Corte giust., 10 luglio 2014, causa C-295/12 P, *Telefónica*, ECLI:EU:C:2014:2062, punto 128.

[36] Per una ricostruzione dei casi antitrust nel settore farmaceutico, v. Commissione europea, *Report from the Commission to the Council and the European Parliament on Competition Enforcement in the Pharmaceutical Sector (2009 – 2017) - European competition authorities working together for affordable and innovative medicines*, Lussemburgo, 2019, nonché il relativo aggiornamento a copertura del periodo 2018-2022. V. anche L. HANCHER, W. SAUTER, *A dose of competition: EU antitrust law in the pharmaceuticals sector,* in *Antitrust Enforcement*, 2016, p. 385; L. HANCHER, *The EU pharmaceuticals market: parameters and pathways,* in E. MOSSIALOS, G. PERMANAND, R. BEATEN, T. HERVEY (a cura di), *Health Systems Governance in Europe, The Role of European Union Law and Policy, European Observatory on Health Systems and Policy*, New York, 2010, p. 635.

[37] Corte giust., 6 dicembre 2012, causa C-457/10 P, *Astrazeneca*, ECLI:EU:C:2012:770, punto 134. Precisa, inoltre, la Corte che: «l'illegittimità di un comportamento abusivo alla luce dell'articolo 82 CE non ha alcuna relazione con la sua conformità o meno ad altre norme giuridiche, e gli abusi di posizione dominante consistono, nella maggioranza dei casi, in comportamenti peraltro legittimi alla luce di branche del diritto diverse dal diritto della concorrenza», punto 132.

conto dei vincoli regolatori propri del settore interessato, quali i regimi di rimborsabilità e autorizzazione dei farmaci[38].

L'orientamento sulla complementarità delle normative in questione, fatto proprio dal legislatore dell'UE e dalla Corte di giustizia, risulta coerente con l'analisi sistematica del diritto dell'Unione europea. In particolare, il diritto della concorrenza e la regolamentazione economica si collocano nel quadro degli obiettivi generali sanciti dall'art. 3, par. 3, TUE e dal Protocollo n. 27 sul mercato interno e la concorrenza, che mirano, in ultima analisi, a garantire il corretto funzionamento del mercato interno. Tale obiettivo orienta, altresì, la scelta delle basi giuridiche per l'adozione del diritto derivato, rispettivamente l'art. 103 TFUE per le misure di attuazione delle norme antitrust e l'art. 114 TFUE per l'armonizzazione delle legislazioni nazionali e, in questa prospettiva, il diritto della concorrenza e la regolamentazione possono essere letti come strumenti integrati della politica economica comunitaria[39].

3. La natura ibrida del *Digital Market Act*

3.1. Indici che riconducono il *Digital Market Act* alla regolamentazione economica

3.1.1. L'ambito di applicazione materiale del DMA

Sulla base della ricostruzione sin qui svolta, è possibile procedere all'analisi della natura del DMA e del suo rapporto con il diritto della concorrenza, chiarendone le linee di continuità e di divergenza.

Innanzitutto, sono molteplici gli indici, tanto formali quanto sostanziali, che permettono di inquadrare il DMA nella categoria della regolamentazione economica.

L'art. 1 DMA delimita il suo ambito applicativo, sotto il profilo oggettivo, ai «servizi di piattaforma di base» ("SPB")[40], strutture multi-

[38] Corte giust., rispettivamente sentenza del 23 gennaio 2018, causa C 179/16, *F. Hoffmann-La Roche e a.*, ECLI:EU:C:2018:25, punti 65 e 80 e sentenza del 30 gennaio 2020, causa C-307/18, *Generics (UK) Ltd.*, ECLI:EU:C:2020:52, punto 40. Sul tema sia consentito il rinvio a M. GUIDI, *Il complesso bilanciamento tra le norme della concorrenza dell'Unione europea e la disciplina regolatoria del settore farmaceutico: il caso Avastin-Lucentis*, in *questa Rivista*, 3/2019, p. 33.

[39] A. DE STREEL, P. LAROUCHE, *The European Digital Markets Act: A Revolution Grounded on Traditions*, cit., p. 543 ss.

[40] Il DMA non prevede una definizione di "servizio di piattaforma di base". Il regolamento si limita, da un lato, a richiamarne nel considerando 2 alcune caratteristiche ricorrenti – senza tuttavia chiarire se esse siano comuni a tutte le tipologie di SPB e se debbano necessariamente coesistere – e, dall'altro, a fornirne un'elencazione tassativa

versante che mediano le interazioni tra gli utenti finali (i consumatori) e gli utenti commerciali (le imprese attive sulla piattaforma) e comprendono, tra gli altri, servizi di intermediazione e ricerca online, *social network*, piattaforme di condivisione video, sistemi operativi, *browser web*, *cloud computing* e pubblicità *online*[41]; sotto il profilo soggettivo, alle imprese designate, ai sensi dell'art. 3, quali «gatekeeper» in riferimento ad uno o più specifici SPB[42].

---

all'art. 2, punto 2. Rientrano in tale categoria: *a*) servizi di intermediazione online; *b*) motori di ricerca online; *c*) servizi di *social network* online; *d*) servizi di piattaforma per la condivisione di video; *e*) servizi di comunicazione interpersonale indipendenti dal numero; *f*) sistemi operativi; *g*) *browser web*; *h*) assistenti virtuali; *i*) servizi di *cloud computing*; *j*) servizi pubblicitari erogati da un fornitore di uno dei servizi di piattaforma di base elencati alle lettere precedenti.". Di contro, sono esclusi «i servizi che agiscono a fini non commerciali, come i progetti di collaborazione». La lacuna del DMA sotto tale profilo è stata oggetto di critiche volte ad evidenziare il ruolo meramente formale del concetto di SPB. Sul punto v. French Minister of State for Digital Transition and Electronic Communications **e** del Dutch Ministry of Economic Affairs and Climate Policy**,** *Considerations of France and the Netherlands regarding intervention on platforms with a gatekeeper position* (2020); European Commission - Regulatory Scrutiny Board opinion, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, SEC(2020) 437/2, 19.1.2021. Per un approfondimento sui SPB, v. G. COLANGELO, *DMA, Begins*, cit., p. 3. N. MORENO BELLOSO, N. PETIT, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, in *European Law Review*, 2023, p. 398 ss.

[41] L'efficienza di tale struttura è connessa alla capacità dell'impresa di bilanciare strategicamente i prezzi tra i due versanti. Infatti, mentre un versante del mercato – caratterizzato da una domanda più elastica o da un maggiore valore attrattivo – viene "sovvenzionato", l'altro versante si fa carico del costo del servizio di intermediazione prestato dalla piattaforma. Tale schema di prezzo asimmetrico caratterizza, ad esempio, la fornitura di servizi pubblicitari online attivi nei mercati dei *social network* e dei motori di ricerca, ove l'accesso gratuito al servizio per i consumatori è compensato dalla monetizzazione delle loro preferenze, che sono cedute a inserzionisti e venditori. Sul tema dei mercati a due o più versanti v. A. DE STREEL, P. LAROUCHE, *The European Digital Markets Act: A Revolution Grounded on Traditions*, in *Journal of European Competition Law & Practice*, 7/2021, p. 542; A. LAMADRID DE PABLO, *The Double Duality of Two-Sided Markets*, in *Competition Law*, 2015, p. 5; B. CAILLAUD, B. JULLIEN, *Chicken and Egg: Competition among Intermediation Service Providers*, in *The RAND Journal of Economics*, 2/2003, p. 309; J.-C. ROCHET, J. TIROLE, *Platform Competition in Two-Sided Markets*, in *Journal of the European Economic Association*, 4/2003, p. 990; D.S. EVANS, *The Antitrust Economics of Multi-Sided Platform Markets*, in *Yale Journal on Regulation*, vol. 20, n. 2, 2003, pp. 325-381; M.L. KATZ, C. SHAPIRO, *Network Externalities, Competition, and Compatibility*, in *American Economic Review*, 3/1985, p. 424.

[42] Per procedere alla designazione di un'impresa quale *gatekeeper*, la Commissione deve adottare una decisione formale ai sensi dell'art. 3 DMA. Tale decisione individua espressamente i SPB forniti dall'impresa che costituiscono, ciascuno, un «importante punto di accesso» per gli utenti commerciali al fine di raggiungere gli utenti finali. Ne consegue che la designazione a *gatekeeper* non riguarda l'impresa in quanto tale, ma

Nello specifico, il sistema di designazione di un'impresa a *gatekeeper* si fonda su tre condizioni cumulative[43]. L'art. 3, par. 1 del DMA prevede che l'impresa in questione: *a*) «ha un impatto significativo sul mercato interno»; *b*) «detiene una posizione consolidata e duratura nell'ambito delle proprie attività o è prevedibile che acquisisca siffatta posizione nel prossimo futuro»; *c*) gestisce un SPB che «costituisce un punto di accesso (gateway) importante affinché gli utenti commerciali raggiungano gli utenti finali». Tali condizioni si presumono realizzate, ai sensi dell'art. 3, par. 2, al raggiungimento di soglie prefissate relative ai volumi di fatturato dell'impresa (lett. a), alla consistenza di utenti finali e commerciali attivi sul SPB (lett. c) e, infine, al consolidamento di tali volumi di utenti per almeno tre esercizi finanziari consecutivi (lett. b)[44].

L'ambito di applicazione materiale è un primo indice della natura regolatoria del DMA, sotto due aspetti: l'applicabilità ai mercati interessati da fallimenti di mercato e la tipologia di intervento asimmetrica verso i *gatekeeper*.

3.1.1.1. L'applicabilità del DMA ai mercati interessati da fallimenti di mercato

Il DMA costituisce un intervento regolatorio iper-settoriale, in quanto concentrato sui soli SPB, *species* del più ampio *genus* «settore digitale», definito quale «settore dei prodotti e dei servizi forniti mediante, o attraverso, servizi della società dell'informazione» (art. 2, n. 4)[45].

Gli SPB sono i servizi digitali più rilevanti dal punto di vista economico, posto che agevolano «gli scambi commerciali transfrontalieri»

---

opera in relazione a uno o più SPB specifici per i quali risultano soddisfatti i requisiti previsti dal regolamento (considerando 29). Sul concetto di *gatekeeper*, v. S. GUIDI, *Before the Gatekeeper Sits the Law. The Digital Markets Act's Regulation of Information Control*, in *European Papers*, 8/2023, p. 405; G. CONTALDI, *La proposta della Commissione europea di adozione del "Digital Markets Act"*, in *Papers di diritto europeo*, 1/2021, p. 73.

[43] Sul processo di designazione di un'impresa a *gatekeeper* v. G. CARATOZZOLO, *The Digital Markets Act in action: analysis of the early practice of the Commission*, cit., p. 143 ss.

[44] Il calcolo degli utenti attivi, che varia a seconda del SPB, avviene secondo le regole stabilite dall'Allegato A del DMA Le soglie previste dal DMA operano unicamente come presunzioni relative. Il loro superamento non determina automaticamente la qualifica di *gatekeeper*, poiché, ai sensi dell'art. 3, par. 5, l'impresa notificante può dimostrare di non soddisfare «in via eccezionale» i requisiti sostanziali di cui all'art. 3, par. 1, pur ricadendo entro i valori quantitativi contemplati dall'art. 3, par. 2.

[45] F. SPORTA CAPUTI, *Il* Digital Market Act *(Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione ex ante dell'abuso di posizione dominante*, cit., p. 77.

e aprono «opportunità commerciali completamente nuove per un elevato numero di imprese nell'Unione a vantaggio dei consumatori» (considerando 1), al punto da essere stati paragonati ad «infrastrutture essenziali» sia dalla dottrina[46] che dalla Corte di giustizia[47].

Gli SPB sono, altresì, quelli maggiormente esposti a problematiche concorrenziali, a causa dei fallimenti di mercato che li caratterizzano, quali «effetti di rete molto forti», «effetti di *lock-in*», «indisponibilità del *multihoming*», «integrazione verticale», «economie di scala estreme», «esistenza di barriere molto alte all'ingresso o all'uscita» e lo sfruttamento di «input chiave», ossia i dati digitali (*consideranda* 2, 3 e 13). Questi fallimenti, seppur comuni ai settori merceologici tradizionali, assumono nel contesto digitale una portata critica, in quanto la loro interazione e combinazione favorisce i primi operatori entrati sul mercato ("*first mover"*), determina la concentrazione del potere economico in capo a poche imprese ("*winner-takes-all*" o "*winner-takes-most*") e innalza barriere che rendono tale potere difficilmente contestabile[48].

Nello specifico, gli effetti di rete diretti si verificano quando il beneficio che un utente trae da un servizio aumenta con il crescere del numero di altri utenti appartenenti alla stessa categoria. Nei *social network*, ad esempio, più ampio è il gruppo con cui ciascun consumatore può interagire, maggiore è l'utilità percepita, che contribuisce ad attrarre, a sua volta, nuovi utenti, innescando un circolo virtuoso[49]. Gli effetti di rete indiretti, invece, derivano dall'interazione tra gruppi di utenti distinti – ad esempio, consumatori e inserzionisti – che traggono un vantaggio

[46] G. MAZZEI, *Big data come beni comuni globali e principi in tema di* public utilities, in *federalismi.it*, 2023, p.162; K.S. RAHMAN, *Regulating informational infrastructure: internet platforms as the new public utilities*, in *Georgetown Law Technology Review*, 2/2018, p. 234.

[47] Cfr. Corte di giustizia, sentenza *Google Search (Shopping)*, cit., punto 224; sentenza del 17 settembre 2007, causa T-201/04, *Microsoft/Commissione*, EU:T:2007:289, punti 208, 388, 390, 421 e 436.

[48] F. MUNARI, *Competition on Digital Markets: An Introduction*, in L. CALZOLARI, A. MIGLIO, C. CELLERINO, F. CROCI, J. ALBERTI (a cura di), *Public and private enforcement of EU competition law in the age of big data*, Torino, 2024, p. 7 ss.; G. CONTALDI, *Il DMA* (Digital Markets Act) *tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani,* 2021, p. 295 ss.; OECD, *Ex ante regulation of digital markets*, cit., p. 9 ss.; J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era*, cit., p. 19 ss.; J. FURMAN ET AL., *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*, cit., p. 17 ss.

[49] J. FARRELL, P. KLEMPERER, *Coordination and Lock-In: Competition with Switching Costs and Network Effects*, in *Handbook of Industrial Organization*, vol. 3, 2007, pp. 1967-207; C. SHAPIRO, H.R. VARIAN (a cura di), *Information Rules: A Strategic Guide to the Network Economy*, Harvard, 1999.

reciproco dall'aumento della consistenza dell'altro gruppo. Seguendo l'esempio del *social network*, un numero crescente di consumatori attira più inserzionisti e editori, i quali ampliano la varietà e la qualità dell'offerta, stimolando a loro volta l'ingresso di nuovi consumatori.

Tali effetti generano barriere all'ingresso, poiché i nuovi operatori, anche se in grado di offrire prodotti o servizi di qualità superiore rispetto al *gatekeeper*, difficilmente riescono a raggiungere la massa critica necessaria per godere di siffatti vantaggi (*incumbency advantage*)[50].

Strettamente connessa agli effetti di rete è la raccolta e l'elaborazione dei dati digitali. I *gatekeeper* acquisiscono, anche mediante tecniche di intelligenza artificiale come *machine learning* e *deep learning*, ingenti quantità di *big data*[51], utilizzandoli per affinare la personalizzazione dei servizi e ampliare la propria offerta. La gestione di tali dati conferisce un

[50] E. GIOVANNETTI, P. SICILIANI, *Platform Competition and Incumbency Advantage under Heterogeneous Lock-in effects*, in *Information Economics and Policy*, 2023, p. 1.

[51] L'espressione "big data" descrive un insieme di dati caratterizzato da un volume, una varietà ed una velocità – le cd. 3 "V" (*Volume*, *Variety*, *Velocity*) – tali da richiedere l'applicazione di algoritmi particolarmente performanti per la loro sistematizzazione ed elaborazione. V. D. LANEY, *3-D data management: controlling data volume, velocity and variety*, in *META Group Research Note*, 2001. A tali caratteristiche se ne sono, in seguito, aggiunte altre, tra cui la cd. "veridicità" che indica l'accuratezza dei dati, intesa nella sua accezione sia microscopica, ossia a livello di singolo dato, sia macroscopica, qualora riferita a *dataset* di grandi dimensioni, o a banche dati interconnesse; la "valenza", ovvero il grado di connessione del dato con altri dati; e, infine, la "visualizzazione", ossia la necessità di riassumere in maniera visuale e facilmente interpretabile i dati più rilevanti e la conoscenza estratta da essi. V. T. SHAFER, *The 42 V's of Big data and Data Science*, in *Elder Research – Data Science & Predictive Analytics*, 2017, p. 1; R. KITCHIN, G. MCARDLE, *What makes Big Data, Big Data? Exploring the ontological characteristics of 26 datasets*, in *Big Data & Society*, 2016, p. 1; S. SUTHAHARAN, *Big Data classification: problems and challenges in network intrusion prediction with machine learning*, in *Performance Evaluation Review*, 2014, p. 70 e ss.; D.E. O'LEARY, *Artificial intelligence and big data*, in *IEEE Intelligent Systems*, 2013, p. 96. Per una prima definizione di "big data" nel diritto dell'UE, v. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 21 gennaio 2015, Verso una florida economia basata sui dati, COM(2014)442 def., p. 5, che li definisce quali «grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti. La gestione di questi dataset ad elevata variabilità e in tempo reale impone il ricorso a nuovi strumenti e metodi, quali ad esempio potenti processori, software e algoritmi»; nonché Article 29 Working Party, *Opinion 03/2013 on purpose limitation*, 2 aprile 2013, WP 203, p. 35, secondo cui i *big data* si riferiscono a «to gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms». V. anche Parlamento europeo, Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto, 2016/2225(INI); European Data Protection Supervisor, *Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy*, 2014, p. 6.

vantaggio competitivo rispetto sia ai clienti che operano in stadi diversi della *big data value chain*, sia ai concorrenti diretti[52]. Il primo scenario si verifica quando i *gatekeeper* sfruttano le informazioni raccolte dagli utenti commerciali nell'ambito del SPB – relative, ad esempio, alle preferenze di acquisto o ai comportamenti di consumo – per offrire beni e servizi in concorrenza con questi ultimi. Il vantaggio per i *gatekeeper* non deriva solo da tale condotta opportunistica, ma anche dal fatto che la loro spinta competitiva si svolge all'interno dell'ambiente digitale dagli stessi regolato tramite condizioni di accesso, di utilizzo e di interruzione del servizio, che li pone in una situazione di vantaggio.

Il secondo scenario, invece, riguarda la difficoltà, per i nuovi entranti, di replicare la disponibilità dei *big data* dei *gatekeeper*, dato che quest'ultimi, grazie agli effetti di rete, possono contare su una più ampia base di utenti, fonte prolifica di dati. Lo sfruttamento di tali dati può combinarsi agli effetti di rete (*data-driven network effect*), alimentandoli ulteriormente, visto che l'aumento degli utenti genera più dati, che

[52] Del tema dei *big data* e i relativi effetti concorrenziali si sono interessate numerose autorità garanti della concorrenza quali: Autoridade da concorrencia, *Digital ecosystems, Big Data and Algorithms - Issues Paper*, 2019; Autorité de la Concurrence, *Contribution de l'Autorité de la concurrence au débat sur la politique de concurrence et les enjeux numériques*, 2019; Japan Fair Trade Commission, *Competition Policy Research Center Report of Study Group on Data and Competition Policy*, 2017; Federal Trade Commission (FTC), *Big Data. A Tool for Inclusion or Exclusion? Understanding the Issues*, 2016; Autorité de la Concurrence, Bundeskartellamt, *Competition Law and Data*, 2016; Monopolkommission, *Competition policy: The challenge of digital markets*, Special Report No. 68, 2015; U.K. Competition and Markets Authority, *The commercial use of consumer data. Report on the CMA's call for information*, 2015. In dottrina v. M. LIBERTINI, *Digital markets and competition policy. Some remarks on the suitability of the antitrust toolkit*, in *Orizzonti del Diritto Commerciale*, 4/2021, p. 337; M. E. CATTANEO, *Big Data*, in A. D. Cortesi (a cura di), *Ict e diritto nella società dell'informazione*, Torino, 2019, p. 175 e ss.; M. MAGGIOLINO, *I big data e il diritto antitrust*, Milano, 2018; B. LASSERRE, A. MUNDT, *Competition law and big data: the enforcers' view*, in *Italian Antitrust Review*, 2017, p. 87; E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*», in *Rivista di diritto dei media*, 6/2017, p. 1; S. VEZZOSO, *Competition policy in a world of big data*, in F. X. Olleros, M. Zhegu (a cura di), *Research Handbook on Digital Transformations*, Cheltenham, 2016; G. PITRUZZELLA, *Big Data, Competition and Privacy: A Look From The Antitrust Perspective*, in *Concorrenza e Mercato*, 2016, p. 15; F. DI PORTO, *La rivoluzione dei big data*, in *Concorrenza e Mercato*, 2016, p. 5; M. STUCKE, A. GRUNES, *Big Data and Competition Policy*, Oxford, 2016; D. SOKOL, R. COMERFORD, *Antitrust and Regulating Big Data*, in *George Mason Law Review*, 2016, p. 1129; D. GERADIN, M. KUSCHEWSKY, *Competition law and personal data: Preliminary thoughts on a complex issue*, in *Concurrences*, 2013, p. 14.

contribuiscono a migliorare a loro volta i servizi, attraendo ulteriori utenti[53].

Si tratta di un fenomeno sostenuto dal cd. *lock-in* dei consumatori, ossia la limitata propensione di quest'ultimi a indirizzarsi a SPB di concorrenti. Tale inerzia può dipendere sia da fattori economici, quali prezzi più elevati dei servizi o beni concorrenti, sia da barriere di natura tecnica o psicologica, come la necessità di apprendere il funzionamento di un nuovo sistema operativo o di ricostruire, da capo, la propria rete sociale ("*switching costs*"). Il *lock-in* tende a rafforzarsi in presenza di restrizioni al *multi-homing* imposte dal *gatekepeer* stesso, vale a dire la possibilità per l'utente di utilizzare contemporaneamente più SPB concorrenti, a causa dell'assenza di interoperabilità tra i rispettivi software e hardware, oppure dell'imposizione di vincoli contrattuali, quali sconti fidelizzanti o pratiche di *tying*.

Il risultato non è solo il consolidamento della base utenti, ma anche il suo confinamento all'interno di veri e propri "ecosistemi", in cui l'offerta di più beni o servizi tra loro interconnessi consente ai *gatekeeper* lo sfruttamento di economie di scala e di scopo ("*portfolio effects*"), restringendo ulteriormente i margini di una competizione effettiva[54]. Infatti, una volta affermatosi l'ecosistema digitale, esso tende ad attrarre progressivamente un'ampia gamma di prodotti e servizi complementari, generando una forza centripeta che favorisce l'affermazione di standard tecnici che limitano l'interoperabilità, incrementando i costi del *multi-homing* e rinforzando il *lock-in* di utenti commerciali e finali[55].

---

[53] Si tratta di una problematica alla quale il legislatore dell'Unione europea ha tentato di far fronte sotto differenti prospettive. In tal senso, infatti, possono leggersi le misure dirette alla portabilità dei dati *ex* artt. 20 GDPR nonché i principi sul cd. *data altruism* e sull'accessibilità ed interoperabilità dei dati previsti, rispettivamente, dai regolamenti *Data Governance Act* e *Data Act*, che mirano a realizzare un mercato comune dei dati.

[54] Le prime si realizzano quando, una volta creata un'infrastruttura digitale, l'aumento esponenziale degli utenti non comporta un corrispondente incremento dei costi, i quali tendono, invece, a ridursi. Le economie di scopo, invece, derivano dall'integrazione verticale e orizzontale di servizi, come nel caso di un motore di ricerca integrato in un sistema operativo o in un *browser web* proprietario, che consente agli utenti di accedere senza soluzione di continuità a una pluralità di servizi (si pensi ai servizi offerti da Alphabet quali il motore di ricerca *Google Search*, il sistema operativo mobile *Android*, il servizio di geolocalizzazione *Maps*, e il servizio di condivisione contenuti video digitali *YouTube*). Sul tema v. M. BOURREAU, *Some Economics of Digital Ecosystems*, DAF/COMP/WD(2020)89, p. 3 ss.

[55] M. CAPPAI, G. COLANGELO, *Taming digital gatekeepers: the 'more regulatory' approach to antitrust law*, p. 9 ss.

Il DMA, dunque, mirando alla risoluzione di specifici fallimenti di mercato di porzioni del settore digitale, testimonia la propria natura di atto di regolamentazione economica.

3.1.1.2. L'intervento asimmetrico nei confronti dei *gatekeeper*

Il DMA chiarisce che «il fatto che un servizio digitale costituisca un servizio di piattaforma di base non solleva di per sé preoccupazioni sufficientemente gravi in termini di contendibilità o di pratiche sleali», le quali emergono, invece, nel caso in cui tale servizio sia prestato da un *gatekeeper* (considerando 15).

Come osservato, il DMA è indirizzato ai *gatekeeper*, ossia le piattaforme online che, grazie al «considerevole potere economico» e all'«impatto significativo sul mercato interno» derivante dal loro ruolo di punti di accesso «a un gran numero di utenti commerciali per raggiungere gli utenti finali in tutta l'Unione e su mercati diversi»[56], sono maggiormente inclini allo sfruttamento dei suddetti fallimenti di mercato degli SPB[57].

Tale approccio asimmetrico risponde, innanzitutto, all'esigenza esplicitata dal DMA di colmare un vuoto normativo in merito alle condotte di *gatekeeper* che, non detenendo una posizione dominante, rischierebbero di sfuggire all'applicazione degli artt. 101 e 102 TFUE[58].

Inoltre, il processo di designazione dei *gatekeeper*, fondato sulle suddette presunzioni legali, consente al DMA di prescindere dai limiti strutturali che l'analisi antitrust incontra nell'accertamento della posizione dominante nei mercati digitali, assumendo che, oltre determinate soglie, alcune piattaforme online presentino una "pericolosità" intrinseca dovuta alla loro capacità di sfruttare i fallimenti di mercato degli SPB[59].

---

[56] Cfr. considerando 6, DMA.

[57] Come specificato dal considerando 24 DMA, in linea teorica anche piccole e medie imprese, pur non raggiungendo le soglie dettate dall'art. 3, par. 2, potrebbe essere designate quali *gatekeeper*, ai sensi del procedimento dettato dall'art. 17 DMA. In questa evenienza, tuttavia, il DMA precisa che la Commissione europea «dovrebbe prendere attentamente in considerazione l'eventualità che tale impresa possa compromettere in modo sostanziale la contendibilità dei servizi di piattaforma di base, in quanto il presente regolamento è destinato principalmente a grandi imprese dotate di considerevole potere economico, piuttosto che a imprese di dimensioni medie o piccole o a microimprese». N. MORENO BELLOSO, N. PETIT, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, cit., p. 391.

[58] Cfr. considerando 5, DMA.

[59] In dottrina, v. F. SPORTA CAPUTI, *Il* Digital Market Act *(Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione ex ante dell'abuso di posizione dominante*, cit., p. 77

Tale scelta deriva dalla consapevolezza che gli strumenti analitici tradizionali del diritto della concorrenza – elaborati con riferimento ai settori "analogici" (*brick-and-mortar*) – risultano inadeguati a cogliere le peculiarità dell'economia digitale. La stessa definizione del mercato rilevante risulta problematica in presenza di piattaforme online strutturate su più versanti, tra loro strettamente interdipendenti (cd. *multi-side market*)[60], e caratterizzate dall'offerta di servizi a titolo gratuito (cd. *zero-price market*). In questo contesto, il test del cd. *Small but Significant and Non-transitory Increase in Price* (SSNIP), cardine della metodologia antitrust tradizionale, diviene inutilizzabile, imponendo alle autorità complesse operazioni di adattamento (come il cd. *Small but Significant and Non-transitory Decrease in Quality*), la cui applicazione rimane tuttavia incerta e difficilmente oggettivabile[61].

3.1.2. L'art. 114 TFUE quale base giuridica del DMA

La scelta della base giuridica del DMA è ricaduta sull'art. 114 TFUE[62]. Si tratta di un'impostazione che, da un lato, esplicita la volontà del legislatore di affiancare il DMA al diritto della concorrenza, senza però integrarlo formalmente, effetto, invece, che si sarebbe potuto realizzare qualora la base giuridica fosse stata individuata nell'art. 103 TFUE[63]; dall'altro lato, è coerente non solo con gli altri atti di regolamentazione

---

ss.; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, cit., p. 31.

[60] J. CREMER, Y. A. DE MONTJOYE, H. SCHWEITZER, *Competition policy in the digital era*, p. 46 ss.; U. FRANCK, M. PEITZ, *Market definition and market power in the platform economy*, *CERRE Report*, 2019, p. 23 ss.; D.S. EVANS, R. SCHMALENSEE, *Markets with Two-Sided Platforms*, in *Issues Competition L. & Policy*, 2008, p. 667; J.C. ROCHET, J. TIROLE, *Platform Competition in Two-sided Markets*, in *J. European Econ. Assn.*, 2003, p. 1015.

[61] OECD, *The Role and Measurement of Quality in Competition Analysis*, cit., p. 15: «[the] idea is therefore probably more useful as a loose conceptual guide than as a precise tool that courts and competition authorities should actually attempt to apply». Sul tema v. anche OECD, *Abuse of dominance in digital markets,* p. 15 ss.; OECD, *Rethinking Antitrust Tools for Multi-Sided Platforms*, 2018, p. 9 ss.

[62] V. A. LAMADRID DE PABLO, N. BAYÓN FERNÁNDEZ, *Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and How to Fix It*, in *Journal of European Competition Law & Practice*, 2021, p. 576; T.M. MOSCHETTA, *Il ravvicinamento delle normative nazionali per il mercato interno. Riflessioni sul sistema delle fonti alla luce dell'art. 114 TFUE*, Bari, 2018.

[63] P. OCCHIUZZI, *Commento all'art. 103 TFUE*, in F. ARENA, R. CHIEPPA (a cura di), *Codice della Concorrenza*, Milano, 2023, p. 75.

finalizzati all'attuazione del Mercato Unico Digitale[64], ma altresì con lo scopo principale del DMA, ossia quello di «contribuire al corretto funzionamento del mercato interno», garantendo che i mercati nel settore digitale siano «equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali» attraverso la previsione di regole uniformi che riducano il rischio di frammentazione a livello di stati membri.

A tal fine, l'art. 1, par. 5, DMA stabilisce che gli Stati membri non possono imporre ai *gatekeeper* obblighi ulteriori rispetto a quelli previsti dal regolamento «al fine di garantire mercati equi e contendibili». Tuttavia, la medesima norma introduce un margine di discrezionalità per gli Stati membri che possono imporre obblighi alle imprese – compresi i fornitori di servizi di piattaforma di base – per condotte che non rientrano nell'ambito di applicazione del DMA, purché tali obblighi siano compatibili con il diritto dell'Unione e non siano correlati allo *status* di *gatekeeper*.

Tale margine di flessibilità è ulteriormente esteso dall'art. 1, par. 6, secondo cui il DMA "*non pregiudica*» l'applicazione non solo della disciplina antitrust dell'UE e nazionale ma anche delle normative nazionali in materia di concorrenza che vietano altre forme di comportamento unilaterale, nella misura in cui esse si applichino anche imprese diverse dai *gatekeeper* o comportino l'imposizione di obblighi ulteriori – rispetto a quelli dettati dal DMA – ai *gatekeeper*. Ne deriva che, sotto il profilo formale, gli Stati membri rimangono liberi di adottare normative che si sovrappongono agli obiettivi del DMA, purché non siano rivolte *esclusivamente* ai *gatekeeper* e ricadano nell'alveo delle competenze nazionali in materia di tutela della concorrenza o di altri obiettivi legittimi d'interesse pubblico[65].

---

[64] V. M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno*? in *Quaderni AISDUE*, Fascicolo speciale n. 2/2024, p. 9.

[65] È in tale contesto che si iscrive la novella legislativa adottata dal legislatore tedesco che ha attribuito all'autorità garante della concorrenza (*Bundeskartellamt*) il potere di imporre divieti e obblighi specifici alle piattaforme che rivestono una «importanza fondamentale per la concorrenza tra i mercati», v. Sezione 19a della normativa a tutela della concorrenza "Gesetz gegen Wettbewerbsbeschränkungen" (GWB). Per un approfondimento, v. I. GRAEF, *Regulating digital platforms: Streamlining the interaction between the Digital Markets Act and national competition regimes*, cit., p. 163 ss.; C. OSTI, *Il* Digital Market Act *tra regolazione e concorrenza*, cit., p. 128 ss.

Questo impianto sistematico si rispecchia nella *governance* del regolamento, prevista dall'art. 38. Nello specifico, l'art. 38, par. 7, stabilisce in favore delle autorità nazionali competenti nell'ambito delle suddette normative nazionali richiamate dall'art. 1, par. 6, un ampio margine di intervento. Sebbene, infatti, la disposizione ribadisca che la Commissione è l'unica autorità preposta all'applicazione del regolamento, essa conferisce alle autorità nazionali il potere di svolgere, di loro iniziativa, un'indagine sui casi di possibile non conformità agli artt. 5, 6 e 7 DMA afferenti al rispettivo territorio, attuando una marcata decentralizzazione nei controlli svolti ai sensi del regolamento[66].

L'esercizio di tali poteri da parte delle autorità nazionali è, tuttavia, limitato sia dall'obbligo di informare la Commissione prima dell'adozione di una misura formale di indagine sia dal potere di avocazione della Commissione, il cui avvio di «un procedimento a norma dell'articolo 20 preclude alle autorità nazionali competenti […] la possibilità di condurre tale indagine o determina la sua conclusione qualora essa sia già in corso».

A tali contrappesi si aggiunge il richiamo dell'art. 38, par. 1, al cd. *European Competition Network* (ECN) di cui alla Direttiva (UE) 2019/1[67], quale sede per lo «scambio reciproco di informazioni» e il «coordinamento delle rispettive azioni», che contribuisce a rafforzare la cooperazione tra la Commissione europea e le autorità nazionali.

3.1.3. Gli obblighi *ex ante* del DMA

La tipologia di obblighi stabiliti dal DMA testimonia la sua natura di atto di regolamentazione economica.

Il DMA impone ai *gatekeeper* un elenco tassativo[68] ed eterogeneo di obblighi che si distinguono sotto un duplice profilo. Mentre gli obblighi previsti dagli artt. 5 e 6 sono applicabili a tutti i *gatekeeper*, invece quelli dettati dall'art. 7 trovano applicazione verso i soli *gatekeeper* che

[66] Si tratta di una struttura di *governance* differente dall'impianto originario, che sconta le pressioni svolte dalle autorità nazionali. V. ECN, *Joint paper of the heads of the national competition authorities of the European Union. How national competition agencies can strengthen the DMA*, del 21 giugno 2021, disponibile online all'indirizzo https://ec.europa.eu/competition/ecn/DMA_joint_EU_NCAs_paper_21.06.2021.pdf.

[67] Direttiva (UE) 2019/1 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che conferisce alle autorità garanti della concorrenza degli Stati membri poteri di applicazione più efficace e che assicura il corretto funzionamento del mercato interno, in *GUUE* L 11 del 14 gennaio 2019, p. 3.

[68] Si tratta di un elenco non suscettibile di estensione, ma solo di aggiornamento, da parte della Commissione, ai sensi della procedura prevista dal combinato disposto dagli artt. 12, 19 e 49.

forniscono servizi di comunicazione interpersonale indipendenti dal numero (quali *WhatsApp, Messenger, Telegram*), definiti dall'art. 2, punto 7, della Direttiva (UE) 2018/1972[69].

Inoltre, sul piano funzionale, l'art. 5 introduce obblighi *self-executing*, la cui applicazione non richiede alcuna attività interpretativa della Commissione. Gli artt. 6 e 7, invece, prevedono obblighi formulati mediante clausole generali che, a discrezione della Commissione europea, possono prevedere un'interlocuzione procedimentalizzata tra quest'ultima e il *gatekeeper* per definirne le modalità concrete di adempimento, secondo quanto stabilito dall'art. 8[70].

Tutti gli obblighi sono accomunati dall'applicabilità *ex ante* che si sostituisce alla «indagine approfondita, caso per caso, di fatti spesso molto complessi», svolta, *ex post*, dalle autorità antitrust (*consideranda* 5 e 10). In tal modo, il DMA intende rimediare, innanzitutto, alle carenze riscontrate dalla prassi antitrust sotto i profili dell'inefficacia dei rimedi comportamentali e della eccessiva durata dei procedimenti istruttori e giurisdizionali, come dimostrato, per entrambi gli aspetti, dal caso *Google Search (Shopping)*.

L'introduzione, da parte di Google, del nuovo sistema di *comparison shopping services* al fine di ottemperare all'obbligo di garantire un trattamento paritario ai servizi concorrenti nei risultati del motore di ricerca, non pare aver ripristinato uno stato di concorrenza effettiva[71]. In

---

[69] Posto che un'impresa è designata quale *gatekeeper* con riferimento a uno o più servizi di piattaforma di base specificamente indicati nella decisione di designazione, ne consegue la sua sottoposizione a soli determinati obblighi e divieti. Ad esempio, un'impresa designata come *gatekeeper* in riferimento al SPB-motore di ricerca online non ricade, per ciò solo, negli obblighi previsti dal regolamento per i SPB-sistemi operativi, a meno che non soddisfi autonomamente i criteri di *gatekeeping* anche per quest'ultimo servizio. V. N. MORENO BELLOSO, N. PETIT, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, cit., p. 402.

[70] In particolare, ai sensi dell'art. 8, par. 2, la Commissione può adottare un atto di esecuzione che specifica le misure che il *gatekeeper* interessato deve attuare per garantire un'osservanza effettiva degli obblighi di cui agli artt. 6 e 7. Inoltre, ex art. 8, par. 3, un *gatekeeper* può richiedere che la Commissione avvii un processo al fine di determinare se le misure che esso intende attuare o ha attuato per garantire la conformità agli artt. 6 e 7 siano efficaci ai fini del conseguimento dell'obiettivo del pertinente obbligo nelle circostanze specifiche del *gatekeeper*. La decisione di aprire, o meno, tale «dialogo con il gatekeeper interessato» è a discrezione della Commissione, che la esercita «nel rispetto dei principi della parità di trattamento, della proporzionalità e della buona amministrazione», cfr. considerando 65 DMA.

[71] Caso AT.39740, parr. 693 ss. Sul caso v. P. AKMAN, *The theory of abuse in Google Search: a positive and normative assessment under EU competition law*, in *Journal of Law, Technology and Policy*, 2017, p. 301.

particolare, è stato messo in rilievo che buona parte del traffico generato dal canale *Google Search (Shopping)* è rimasta appannaggio di servizi riconducibili a *Google* stessa, a discapito dei concorrenti[72].

Inoltre, nonostante l'indagine della Commissione sia stata avviata nel 2010, il procedimento si è concluso solamente nel 2024; periodo durante il quale le pratiche contestate hanno prodotto effetti irreversibili sul mercato, quali il fallimento della società *Foundem*, tra i primi denuncianti, a dimostrazione del rischio concreto che la durata eccessiva dei procedimenti vanifichi l'efficacia deterrente e ripristinatoria dell'antitrust[73], a cui contribuisce, per altro verso, lo scarso utilizzo dell'art. 8 del Regolamento n. 1/2003 in materia di applicazione di misure provvisorie[74].

---

[72] A tal proposito possono riportarsi tanto l'audizione parlamentare della Commissaria alla Concorrenza M. Vestagher tenutasi il 19 novembre 2019 (cfr. European Parliament, Parliamentary questions, 19 November 2019, disponibile https://www.europarl.europa.eu/doceo/document/E-9-2019-003869_EN.html), quanto l'analisi svolta dall'associazione di consumatori a livello europeo (BEUC, Consumer concerns over Google Shopping remedies, Policy Report, 2020). Sul tema v. R. FEASEY, J. KRÄMER, *Implementing effective remedies for intermediation bias*, CERRE Report, 2019; B. VESTERDORF, K. FOUNTOUKAKOS, *An Appraisal of the Remedy in the Commission's Google Search (Shopping) Decision and a Guide to its Interpretation in Light of an Analytical Reading of the Case Law*, in *Journal of European Competition Law & Practice*, 1/2018, p. 3.

[73] Corte giust., 10 settembre 2024, causa C-48/22 P, *Google Search (Shopping)*, ECLI:EU:C:2024:726, per un primo commento sulla quale si rimanda a E. FISCHER, L. HORNKOHL, N. IMGARTEN, *Discriminatory Leveraging Plus: The Standard for Independent Self-Preferencing Abuses after Google Shopping (C-48/22 P)*, in *European Papers,* 1/2025, p. 25. Sul tema della lentezza dei procedimenti antitrust **v.** E.A. RAFFAELLI, *I mercati digitali e le norme di regolazione: tra limiti del diritto antitrust e nuove modalità di intervento* ex ante, cit., p. 54. Tale problematica è stata, altresì, identificata da Commission Staff Working Document - Impact Assessment Report Accompanying the document Proposal for a regulation on contestable and fair markets in the digital sector (Digital Markets Act) SWD(2020) 363 def., p. 119. In tale prospettiva può citarsi anche il caso *Google Android*, iniziato nel 2013, quando la *FairSearch AISBL*, associazione che riunisce imprese operanti nel settore delle tecnologie dell'informazione e della comunicazione, ha presentato una denuncia alla Commissione europea riguardo a specifiche pratiche commerciali adottate da Google nel segmento dell'Internet mobile. In seguito a tale denuncia, la Commissione ha rivolto richieste di informazioni a Google, ai suoi clienti, ai concorrenti e ad altri operatori del settore. Il 15 aprile 2015 la Commissione ha quindi avviato un procedimento formale in relazione al sistema operativo Android. Il contenzioso è, tuttora, pendente dinnanzi alla Corte di giustizia (causa C-738/22 P - *Google and Alphabet v Commission*).

[74] V. Commission Staff Working Paper, *Evaluation of Regulation 1/2003* and 773/2004, SWD(2024) 216 def., in cui si sottolinea che dall'adozione del regolamento n. 1/2003 ad oggi, le misure provvisorie ai sensi dell'art. 8 del regolamento n. 1/2003 sono state imposte solo una volta, ossia nel caso *Broadcom* (Commissione europea, *Decisione*

L'applicazione automatica degli obblighi consente, infine, di far fronte alle difficoltà della disciplina antitrust nella formulazione di nuove teorie del danno o nel loro adattamento al contesto digitale. Come noto, la teoria del danno costituisce lo strumento analitico attraverso cui è dimostrata l'anti-concorrenzialità di una condotta, colmando la citata portata generica delle clausole normative, attraverso il riferimento a categorie concettuali della scienza economica. Infatti, le clausole generali – come il divieto di abuso di posizione dominante *ex* art. 102 TFUE – la cui portata precettiva è ampia e indeterminata, sono specificati tramite l'utilizzo di concetti quali, ad esempio, "sconti fedeltà", "prezzi predatori", "pratiche di esclusione", volti ad esaminare gli effetti concreti delle pratiche sottoposte a scrutinio antitrust. In questo contesto, la scienza economica, attraverso l'elaborazione di teorie del danno, fornisce dunque il supporto teorico per definire la dannosità di una condotta, dal punto di vista concorrenziale, e sostenere l'attuazione delle norme antitrust e delle relative sanzioni. Nel caso dei mercati digitali, questa prassi si è scontrata con la difficoltà di dimostrare gli effetti economici escludenti o di sfruttamento (in ossequio al cd. *more economic approach*[75]) rispetto a quelli pro-competitivi, peraltro con riferimento a mercati sorti

AT.40462 – Broadcom, Interim measures, 16 ottobre 2019), sul quale si rimanda a D. MANTZARI, *Interim Measures in EU Competition Cases: Origins, Evolution and Implications for Digital Markets*, CLES Research Paper Series 1/2020. Per una disamina dell'art. 8 regolamento 1/2003 in relazione alle misure provvisorie previste dall'art. 24 DMA v. C. FARINHAS, *Interim Measures in Digital Markets: Interaction Between the DMA and Regulation 1/2003*, in *Utrecht Law Review*, 2/2025, p. 111. Sul tema dell'applicazione di tali misure, v. OECD, *Interim Measures in Antitrust Investigations*, OECD Competition Policy Roundtable Background Note, 2022.

[75] J. BLOCKX, *The Limits of the 'More Economic' Approach to Antitrust*, in *World Competition*, 2019, p. 475; P. IBÁÑEZ COLOMO, *Beyond the 'more economics-based approach': a legal perspective on Article 102 TFEU case law*, in *Common Market Law Review*, 3/2016. p. 709. Sull'importanza della valutazione degli effetti di concotte anticompetitive si è espressa, in più occasioni, la Corte di giustizia, secondo cui: «quando l'impresa in questione sostiene che il suo comportamento non poteva avere effetti anticoncorrenziali, neppure potenziali, e sostiene i suoi argomenti con elementi riguardanti l'evoluzione reale del mercato, spetta all'autorità garante della concorrenza esaminare se detti elementi siano tali da avere un impatto sulla sua valutazione dell'esistenza di effetti anticoncorrenziali. Infatti, nel caso di pratiche effettivamente attuate e che presentano, come nel caso di specie, un carattere complesso, tali elementi possono costituire circostanze pertinenti in grado di corroborare o meno l'esistenza di una violazione dell'articolo 102 TFUE»; Corte giust., *Google and Alphabet v Commission (Google Shopping)*, cit., punto 440. Allo stesso modo, Corte giust., 15 marzo 2007, causa C-95/04 P, *British Airways/Commissione*, EU:C:2007:166, punto 86, e Corte giust., 6 settembre 2017, causa C-413/14 P, *Intel*, ECLI:EU:C:2017:632, punti 139 e 140.

repentinamente e soggetti a continue evoluzioni[76]. Ne consegue che, sebbene, in astratto, lo strumentario applicativo del diritto antitrust si presti ad essere interpretato in modo evolutivo, in dottrina[77] e, soprattutto, nella giurisprudenza della Corte di giustizia[78], tale adattamento non è stato privo di ostacoli.

3.1.4. Transitorietà ed eccezioni di natura economica

Il carattere transitorio del DMA emerge in modo esplicito dall'art. 53, par. 2, che impone alla Commissione di valutare periodicamente – la prima volta entro il 3 maggio 2026 e successivamente ogni tre anni – l'attuazione e l'efficacia del regolamento, tenendo conto, tra l'altro, del livello di contendibilità ed equità dei mercati digitali, dell'impatto sugli utenti finali e commerciali e dell'evoluzione tecnologica (considerando 105).

Si tratta di una clausola che riflette la natura non definitiva del DMA, in linea con la sua logica di intervento regolatorio che trova fondamento nell'esigenza di correggere squilibri contingenti e che, per sua stessa vocazione, è destinato a essere rimodulato o superato una volta venute meno le ragioni che ne hanno giustificato l'adozione.

Accanto a questa clausola di revisione generale, il regolamento introduce una serie di strumenti volti a garantire la continua adattabilità del quadro normativo all'evoluzione dei mercati digitali: il riesame dello status di *gatekeeper* (art. 4), l'aggiornamento dell'elenco dei servizi di piattaforma di base mediante atti delegati (art. 17), l'adozione di atti di esecuzione sulle modalità applicative degli obblighi (art. 20), gli strumenti

[76] International Competition network, *Report on the Results of the ICN Survey on the Analysis of Theories of Harm and the Design of Remedies Concerning Unilateral Conduct With Dominance/Substantial Market Power in Digital Markets*, 2023, p. 10, in cui si sottolinea che: «The survey sought to understand whether ICN member authorities faced specific challenges in applying theories of harm in digital markets. In 17 out of 41 cases, the responding authorities (nine out of 19) said that they faced such challenges.»

[77] Esemplificativa, in tal senso, è la pratica del cd. *self-preferencing*, il cui inquadramento tra le fattispecie di abuso di posizione dominante è stato oggetto di critica, per via dei suoi effetti pro-competitivi. V. F. GHEZZI, M. MAGGIOLINO, *Considerazioni intorno al provvedimento dell'Autorità garante della concorrenza nel caso FBA Amazon: nulla di nuovo sotto il sole?*, in *Riv. regol. merc.*, 1/2022, p. 478; E. DEUTSCHER, *Google Shopping and the Quest for a Legal Test for Self-preferencing Under Article 102 TFEU*, in *European Papers*, 3/2021, 3, p. 1345; P. IBANEZ COLOMO, *Self-preferencing: Yet Antother Ephitet in Need of Limiting Principles*, in *World Competition*, 2020, p. 417; J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Era*, p. 65 ss.

[78] V. Corte giust., 14 settembre 2022, causa T-604/18, *Google Android*, ECLI:EU:T:2022:541; Corte Giust, 15 giugno 2022, causa T-235/18, *Qualcomm*, ECLI:EU:T:2022:358.

di indagine di mercato (artt. 19 e 41) e le relazioni annuali sull'applicazione del regolamento (art. 35).

Tali disposizioni svolgono la funzione – richiamata dai considerando 30 e 77 – di prevenire l'obsolescenza del quadro regolatorio di fronte ai rapidi mutamenti del settore digitale.

Inoltre, l'impianto del DMA non prevede margini di giustificazione basati su efficienze economiche o vantaggi pro-competitivi, come avviene, invece, nell'ambito dell'art. 101, par. 3, e dell'art. 102 TFUE[79]. Sebbene, in via eccezionale, l'art. 9 del DMA consenta alla Commissione di sospendere, per un periodo determinato, l'applicazione di specifici obblighi previsti dagli artt. 5, 6 e 7 qualora «circostanze eccezionali» ne compromettano gravemente la sostenibilità economica o impediscano l'adempimento degli obblighi, tale previsione non introduce una "difesa di efficienza" in senso antitrust, ma un rimedio di carattere straordinario e temporaneo, applicabile solo in presenza di condizioni «indipendenti dalla volontà del *gatekeeper*».

Tale impostazione è coerente con la logica regolatoria del DMA, posto che le valutazioni sulle efficienze e sugli effetti delle condotte sono state svolte *ex ante* dal legislatore, a seguito del bilanciamento dei rischi e benefici immanenti a ciascun obbligo da esso previsto, come emerge sotto due profili. In prima battuta, il DMA specifica che le sue disposizioni si applicano «indipendentemente dagli effetti reali, potenziali o presunti sulla concorrenza in un dato mercato derivanti dal comportamento di un dato *gatekeeper*»[80]. In seconda battuta, il regolamento esclude espressamente la rilevanza di giustificazioni di natura economica per la designazione del *gatekeeper*. Infatti, pur potendo un'impresa confutare – anche in questo caso in «circostanze eccezionali» – la presunzione di avere un impatto significativo sul mercato interno, a tal fine «non dovrebbero essere prese in considerazione giustificazioni per motivi economici basate sulla definizione del mercato o volte a dimostrare efficienze derivanti da un tipo specifico di comportamento dell'impresa che fornisce servizi di piattaforma di base» in quanto, specifica il DMA, «non sono pertinenti per la designazione come *gatekeeper*»[81].

[79] Sul tema delle giustificazioni nell'ambito dell'art. 102 TFUE, v. P. MANZINI, *Diritto antitrust dell'Unione europea*, Torino, 2022, p. 191.
[80] Cfr. Considerando 11, DMA.
[81] Cfr. considerando 23, DMA.

4. Analogie tra il *Digital Market Act* e il diritto della concorrenza

4.1. Analogie sotto il profilo degli obiettivi

A dispetto dei suddetti elementi che permettono di inquadrare il DMA quale atto di regolamentazione economica, altre caratteristiche paiono assimilarlo all'alveo del diritto della concorrenza, lasciando trasparire la sua natura di normativa ibrida[82].

Può leggersi in tale prospettiva l'obiettivo del DMA di garantire «l'equità e la contendibilità» dei SPB prestati dai *gatekeeper*[83], endiadi specificata dal regolamento stesso.

Nello specifico, l'equità viene declinata a contrario, quale negazione della pratica sleale che crea «squilibrio tra i diritti e gli obblighi degli utenti commerciali in cui il gatekeeper trae un vantaggio sproporzionato» e, in tal modo, impedisce agli utenti commerciali di cogliere i vantaggi derivanti dai propri investimenti in innovazione, in quanto costretti a subire le condizioni sfavorevoli imposte dal *gatekeeper* stesso per la fruizione dei servizi di piattaforma di base (considerando 33)[84].

La contendibilità, invece, è definita come la «capacità delle imprese di superare efficacemente le barriere all'ingresso e all'espansione e di contestare il *gatekeeper* per quanto riguarda il merito dei rispettivi prodotti e servizi» (considerando 32), che è limitata dalle caratteristiche «dei servizi di piattaforma di base nel settore digitale, quali effetti di rete, forti economie di scala e vantaggi derivanti dai dati».

Il DMA precisa che l'obiettivo di garantire «l'equità e la contendibilità» dei mercati digitali è «complementare, ma diverso, alla protezione della concorrenza non falsata su un dato mercato, quale definita in termini di diritto della concorrenza»[85]. Tuttavia, i concetti di equità e contendibilità paiono potersi interpretare alla stregua dei concetti di parità di opportunità e di condizioni per tutti i contendenti del mercato, pilastri del più ampio concetto di concorrenzialità che premia gli operatori

---

[82] N. MORENO BELLOSO, N. PETIT, *The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove*, cit., p. 391; 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*, 2022, p. 87; P. LAROUCHE, A. DE STREEL, *The European Digital Markets Act: A Revolution Grounded on Traditions*, cit., p. 542;

[83] F. SPORTA CAPUTI, *Il* Digital Market Act *(Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione ex ante dell'abuso di posizione dominante*, cit., p. 77;

[84] L.J. HOFFMANN, *Fairness in the Digital Markets Act*, in *European Papers*, 1/2023, p. 17; A. LAMADRID DE PABLO, N. BAYÓN FERNÁNDEZ, *Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and How to Fix It*, cit., p. 11.

[85] Cfr. considerando 11, DMA.

economici più meritevoli.

Ciò pare confermato dal DMA stesso il quale, al considerando 107, precisa che l'obiettivo dell'equità e contendibilità dei SPB deve essere interpretato «nell'ottica di promuovere l'innovazione, l'elevata qualità dei prodotti e dei servizi digitali, prezzi equi e concorrenziali, nonché un'elevata qualità e un'ampia scelta per gli utenti finali nel settore digitale», corollari del diritto della concorrenza[86].

Si tratta di un'interpretazione valorizzata dal tenore letterale dell'art. 1, par. 6, in cui si specifica che il DMA, pur lasciando impregiudicati gli artt. 101 e 102 TFUE e le rispettive norme nazionali, «mira a integrare l'applicazione del diritto della concorrenza».

4.2. Analogie sotto il profilo della codificazione della prassi antitrust

Mentre, come osservato, gli obblighi previsti dal DMA hanno caratteristiche di tipo regolatorio, tuttavia, il loro contenuto sostanziale non si limita – come nel citato caso dei servizi aeroportuali – a riflettere la logica sottesa a precedenti interventi antitrust, ma positivizza la prassi decisionale maturata negli ultimi due decenni nell'applicazione degli artt. 101 e 102 TFUE ai mercati digitali[87].

Concentrando l'analisi sulle fattispecie oggetto di provvedimenti da parte sia della disciplina antitrust sia del DMA[88], relativamente agli obblighi *self-executing*, l'art. 5, par. 2, prevede il divieto dei *gatekeeper* di

---

[86] Sul punto G. COLANGELO, *DMA, Begins*, cit., p. 4; P. MANZINI, *Equità e contendibilità nei mercati digitali: la proposta di* Digital Market Act, cit., p. 40.

[87] Il cd. *Impact Assessment* che accompagna la proposta del DMA richiama le indagini antitrust passate e in corso come "evidenza" della scelta delle obbligazioni inserite (Commission Staff Working Document - Impact Assessment Report Accompanying the document Proposal for a regulation on contestable and fair markets in the digital sector (Digital Markets Act) SWD(2020) 363def., pp. 53-60) e, allo stesso modo, il considerando 33 della proposta della Commissione afferma che gli obblighi «*corrispondono a pratiche rispetto alle quali l'esperienza acquisita, ad esempio nell'applicazione delle norme di concorrenza dell'UE, mostra che producono effetti particolarmente negativi*» sugli utenti commerciali e finali. Sul punto, come ricordato da Margrethe Vestager nel discorso "*Competition policy: where we stand and where we're going***"** (Bruges, 25 marzo 2022), "*the development of the DMA has not been happening in a vacuum. Our enforcement in digital markets and the in-depth market knowledge built through case practice enabled us to table the DMA*".

[88] Per una ricostruzione degli obblighi e divieti v. F. SPORTA CAPUTI, *Il* Digital Market Act *(Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione ex ante dell'abuso di posizione dominante*, cit., p. 80 ss.; P. AKMAN, *Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, cit., p. 94.

combinare i dati personali dei propri utenti finali, tra più SPB, o tra questi ed altri servizi, senza il loro consenso. Tale divieto ha lo scopo di evitare che i *gatekeeper* creino barriere all'ingresso consistenti nell'accumulo di dati ricavati dalla loro attività di intermediazione.

Il divieto in questione ruota attorno al concetto di consenso che, mutuato dagli artt. 4, punto 11) e 6. par. 1, lett. a) del Regolamento (UE) 2016/679[89], offre agli utenti finali un controllo più incisivo sulle modalità di utilizzo dei loro dati personali[90], e mira a garantire agli utenti commerciali un migliore accesso a tali dati quando da essi stessi generati nell'ambito dei servizi di piattaforma di base, a tutela del loro ruolo nella citata *big data value chain*.

La disposizione in analisi discende direttamente dal caso *Facebook/Bundeskartellamt*, in materia di intersezione tra tutela della concorrenza e protezione dei dati personali[91]. Nello specifico, la vicenda ha preso avvio con il provvedimento adottato dall'Autorità antitrust tedesca[92] e oggetto di successivo esame da parte tanto della Corte federale

[89] 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), in *GUUE* L 119 del 4 maggio 2016, p. 1. Sul tema v. G.M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *Commentario GDPR e Normativa Privacy*, Milano, 2022; F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. CAVALLO PERIN, D.U. GALETTA (a cura di), *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, 2022, p. 43 ss.; A. PALLOTTA, *Regolamento europeo n. 679/2016: profili di continuità e aspetti innovativi,* in *Eurojus - Fascicolo speciale* "*Mercato Unico Digitale, dati personali e diritti fondamentali*", 2020, p. 95.

[90] Se tale consenso è negato o revocato, il *gatekeeper* può riproporre la richiesta solo una volta all'anno per la stessa finalità.

[91] Sul tema v. I. GRAEF, *Regulating digital platforms: Streamlining the interaction between the Digital Markets Act and national competition regimes*, in I. GRAEF, B. VAN DER SLOOT (a cura di), *The legal consistency of technology regulation in Europe*, Oxford, 2024, p. 162 ss.; I. GRAEF, B. VAN DER SLOOT, *Collective Data Harms at the Crossroads of Data Protection and Competition Law: Moving Beyond Individual Empowerment*, in *European Business Law Review*, 4/2022, p. 513; C. OSTI, R. PARDOLESI, *L'antitrust ai tempi di Facebook*, in *Mercato Concorrenza Regole*, 2/2019, p. 195.

[92] W.P.J. WILS, *The obligation for the competition authorities of the EU Member States to apply EU antitrust law and the Facebook decision of the Bundeskartellamt,* in *Concurrences*, n. 3, 2019; G. COLANGELO, M. MAGGIOLINO, *Big data, data protection and antitrust in the wake of the bunderskartellamt case against Facebook,* in *Italian Antirust Review*, 2017, p. 104.

di giustizia tedesca[93] quanto, in via pregiudiziale, della Corte di giustizia dell'Unione europea[94].

In particolare, il caso ha riguardato la pratica adottata da *Facebook* (oggi *Meta*) di combinare, in violazione del diritto all'autodeterminazione informativa dell'utente, i dati personali raccolti direttamente tramite il proprio *social network* con quelli resi disponibili da altri suoi servizi, quali *Instagram* e *WhatsApp*, nonché da siti *web* o *App* mobili di terze parti, integrati ai primi da meccanismi quali "*like button*" o "*Facebook pixel*" (cd. *Facebook Business Tools*). Dal punto di vista concorrenziale, il Bundeskartellamt ha sostenuto che l'accumulo e l'integrazione illegittima di dati personali, alla base dei servizi di profilazione e di *targeting* promozionale, rafforzasse il potere di mercato di Facebook nel settore della pubblicità *online*, consolidando le barriere all'ingresso e ostacolando la contendibilità del mercato. Sulla base di tali considerazioni, l'autorità tedesca ha qualificato la condotta quale abuso di posizione dominante ai sensi legge antitrust nazionale e dell'art. 102 TFUE.

La riconducibilità di questo caso antitrust all'art. 5, par. 2, DMA è confermata dal procedimento avviato, dalla Commissione europea, sul modello "*Consent or Pay*" di *Meta*. Si tratta, secondo quanto emerso dal *Compliance Report di Meta* – redatto dal *gatekepeer* in questione *ex* art. 11 DMA[95] – di un'alternativa binaria al godimento, da parte degli utenti finali, dei suoi servizi di *social networking*: da un lato, il consenso

---

[93] Sentenza emessa a seguito dell'impugnazione della decisione di primo grado emessa dal Tribunale di Düsseldorf (Oberlandesgericht Düsseldorf, sentenza del 26 agosto 2019, VI-Kart 1/19 (V), WRP 2019, 1333).

[94] Corte giust., 4 luglio 2023, causa C-252/21, *Meta Platforms e a./Bundeskartellamt*, ECLI:EU:C:2023:537. La Corte ha precisato che*:* «*tenuto conto dei diversi obiettivi perseguiti dalle norme stabilite in materia di* concorrenza, in particolare dall'articolo 102 TFUE, da un lato, e da quelle previste in materia di protezione dei dati personali in forza del [GDPR], dall'altro, occorre constatare che, quando un'autorità nazionale garante della concorrenza rileva una violazione di questo regolamento nell'ambito della constatazione di un abuso di posizione dominante, essa non si sostituisce alle autorità di controllo.» Sul tema del potenziale conflitto di competenze tra Autorità garanti della concorrenza e Garante della Privacy si è recentemente espresso lo stesso European Data Protection Board (EPBD), v. EDPB, Position paper on Interplay between data protection and competition law, 16 gennaio 2025*; G.* D'IPPOLITO, *Data economy: la Corte di giustizia precisa il rapporto tra concorrenza e protezione dei dati personali e le norme sulla pubblicità personalizzata,* in *MediaLaws - Rivista del Diritto dei Media, 2/2023, p. 323.*

[95] Ai sensi dell'art. 11 DMA i *gatekeeper* devono trasmettere alla Commissione europea una relazione di conformità che illustri in modo dettagliato e trasparente le misure adottate per assicurare il rispetto degli obblighi previsti dagli artt. 5, 6 e 7, nonché pubblicare e comunicare alla Commissione una sintesi non riservata di tale relazione. Tali sintesi sono pubblicate in una sezione dedicata del sito internet sul DMA implementato dalla Commissione europea https://digital-markets-act.ec.europa.eu/index_en.

al trattamento e alla combinazione dei dati personali tra i diversi servizi Meta quale contropartita ad essere destinatari delle campagne promozionali personalizzate svolte su *Facebook* e *Instagram*; oppure, dall'altro lato, in caso di diniego a tale trattamento, il pagamento di un abbonamento mensile per il godimento di un servizio privo di pubblicità.

La Commissione europea, con decisione del 23 aprile 2024[96], ha accertato che tale modello viola l'art. 5, par. 2, DMA, in quanto non offre agli utenti finali la «scelta specifica» prevista dalla norma, ossia la possibilità di accedere a un servizio che utilizzi meno dati personali, ma che sia equivalente a quello a pagamento (*consideranda* 36 e 37 DMA). La Commissione ha, pertanto, irrogato a *Meta* un'ammenda di 200 milioni di euro ai sensi dell'art. 30 DMA[97], ribadendo un'impostazione che, pur collocandosi nel quadro *ex ante* del regolamento, riprende la logica già valorizzata dal provvedimento antitrust del Bundeskartellamt. In entrambi i casi, l'assenza di un consenso valido costituisce non solo una violazione della disciplina sui dati personali, bensì anche il presupposto della creazione di un vantaggio competitivo indebito (nella prospettiva antitrust) e della distorsione strutturale dell'equità e della contestabilità del mercato dei *social network* (nella prospettiva del DMA)[98].

---

[96] Commissione europea, decisione del 23 aprile 2024, DMA.100055 - *Meta* - Article 5(2).

[97] Nel novembre 2024, a seguito di numerosi scambi con la Commissione, Meta ha introdotto una nuova versione del modello "*free personalised ads*", che offre agli utenti un'opzione presumibilmente basata su un minor utilizzo dei dati personali. La Commissione ha chiarito che la valutazione di tale nuovo modello è ancora in corso, posto che la decisione adottata riguarda esclusivamente il periodo precedente e si fonda sull'analisi di pratiche già attuate dal *gatekeeper*.

[98] Ad ulteriore riprova dell'importanza dei dati digitali e, in particolare, degli interessi degli utenti finali in materia di protezione dei dati e di privacy, il DMA prevede, all'art. 15, l'obbligo per i *gatekeeper* di presentare alla Commissione europea «una descrizione sottoposta a audit indipendente delle tecniche di profilazione dei consumatori» impiegate nell'ambito dei propri servizi di piattaforma di base. Tale descrizione deve contenere informazioni sulla tipologia dei dati personali utilizzati, il trattamento svolto, lo scopo, la durata, l'impatto sui servizi del *gatekeeper,* nonché i provvedimenti adottati tanto «per consentire effettivamente agli utenti finali di essere a conoscenza dell'uso pertinente di tale profilazione», quanto «per chiedere il loro consenso o a offrire loro la possibilità di negare o revocare il consenso». Tale descrizione è sottoposta al comitato europeo per la protezione dei dati per finalità informative ed è, altresì, resa pubblica e aggiornata con cadenza annuale. Precisa, infatti, il DMA che la trasparenza agevola la contendibilità dei servizi di piattaforma di base, esercitando su di essi una pressione esterna allo scopo, da un lato, di evitare il rischio che «la profilazione approfondita dei consumatori» si consolidi quale standard del settore, «dato che i potenziali concorrenti o le start-up non possono accedere ai dati in una misura e con un'accuratezza analoghe, né su una scala paragonabile»; e, dall'altro lato, per consentire «alle altre imprese che forniscono servizi

Il parallelismo con la prassi antitrust riguarda, inoltre, l'art. 5, par. 3, del DMA che vieta l'utilizzo, da parte dei *gatekeeper*, delle cd. clausole di parità ("*price parity clauses*" o "*Most Favored Nation clauses*" - "MFN"), ossia condizioni imposte agli utenti commerciali per impedire loro di offrire, al di fuori del SPB, beni o servizi agli utenti finali, a condizioni migliorative, di prezzo o di altra natura, rispetto a quelle da essi applicate sul SPB stesso.

Nello specifico, le clausole MFN si distinguono tra ampie ("*wide*"), che vietano agli utenti commerciali di offrire condizioni più favorevoli su qualsiasi altro canale (inclusi canali terzi o offline), e ristrette ("*narrow*"), che limitano, invece, il divieto al solo canale diretto dell'utente commerciale come, ad esempio, il suo sito *web*.

Le clausole MFN "*wide*" risultano maggiormente critiche sotto il profilo concorrenziale, poiché tendono a favorire un allineamento generalizzato dei prezzi tra più canali e, al contempo, comprimono i margini di profitto degli utenti commerciali, con ripercussioni direttamente sul prezzo finale ai consumatori. Le clausole MFN "*narrow*", pur potendo ridurre la pressione concorrenziale sul prezzo nei canali diretti gestiti dall'utente commerciale, in taluni contesti, tuttavia, costituiscono un freno al *free riding*, ossia il comportamento opportunistico di quest'ultimo che, godendo della visibilità ottenuta tramite il SPB, offre i propri servizi direttamente al consumatore per evitare il pagamento al *gatekeeper* del prezzo per il servizio di intermediazione ricevuto[99].

Rispetto all'approccio più ondivago delle autorità antitrust verso le clausole *narrow*[100], il DMA ha adottato una scelta più netta che, all'art. 5, par. 3, impone un divieto generalizzato all'impiego di tutte le tipologie di clausole di parità, incluse le pratiche equivalenti che abbiano per oggetto

---

di piattaforma di base di differenziarsi meglio attraverso l'uso di maggiori garanzie della privacy» (considerando 72). V. OECD, *Data portability, interoperability and digital platform competition*, 2021.

[99] Sul tema delle clausole MFN v. G. COLANGELO, *Le* price parity clauses *tra analisi economica e cattura regolatoria*, in *Orizzonti del Diritto Commerciale*, 3|2023, p. 714.

[100] In Italia, v. AGCM, Provv. n. 25422, 21 aprile 2015, *Mercato dei servizi turistici-prenotazioni alberghiere on line*; in Germania, v. Bundeskartellamt, Decisione B9-66/10, 20 dicembre 2013, *"Best Price" clauses of HRS hotel portal violate competition law*; Bundeskartellamt, Decisione B9-121/13, 22 dicembre 2015, *Booking.com*; Bundesgerichtshof, 18 maggio 2021, Caso KVR 54/20, *Booking.com*. In Francia, v. Autorité de la Concurrence, decisione n. 15-D-06, 21 aprile 2015, *Booking.com*; in Svezia, v. Konkurrensverket, decisione n. 596/2013, 15 aprile 2015, *Booking.com* e decisione n. 595/2015, 10 maggio 2015, *Expedia*; in UK v. CMA, Decisione CA98, 16 settembre 2015, *Hotel online booking investigation*.

o effetto quello di impedire la differenziazione delle condizioni commerciali tra canali distributivi, quali l'aumento selettivo delle commissioni o la riduzione della visibilità nei risultati dei motori di ricerca, a discapito degli utenti commerciali.

In attuazione del citato art. 11 DMA, *Booking.com* ha notificato alla Commissione europea l'aggiornamento delle proprie condizioni generali, specificando di aver rimosso le clausole di parità tariffaria e di aver escluso l'utilizzo dei prezzi praticati al di fuori della piattaforma come parametro di riferimento per i propri programmi di fidelizzazione[101].

La tutela prestata agli utenti commerciali è ulteriormente rafforzata dalle previsioni di cui al seguente art. 5, par. 4 (cd. obbligo "*anti-steering*").

Tale disposizione trova il proprio referente teorico nel caso antitrust *App Store Practices (music streaming)*, relativo al mercato della fornitura di applicazioni musicali dirette agli utenti di *iPhone* e *iPad*[102]. In tale ambito, la Commissione ha ritenuto che la condotta di *Apple* di imporre agli sviluppatori di *App* di musica in *streaming* il divieto di informare i consumatori dell'esistenza di abbonamenti acquistabili al di fuori dell'*App Store* e di indirizzarli ("*steering*") verso tali offerte, integrasse un abuso di posizione dominante ai sensi dell'art. 102 TFUE.

Allo stesso modo, ai sensi dell'art. 5, par. 4 DMA, il *gatekeeper* è tenuto a consentire agli utenti commerciali di svolgere, a titolo gratuito e al di fuori della piattaforma, attività promozionale e di vendita di beni o servizi indirizzate agli utenti finali «a prescindere dal fatto che, a tal fine, essi si avvalgano dei servizi di piattaforma di base del *gatekeeper*». Anche nel contesto applicativo del DMA tale disposizione ha assunto rilevanza nel mercato delle *App* mobili, ambito nel quale, ai sensi dell'art. 29 del DMA, la Commissione europea ha avviato, in data 25 marzo 2024, un'indagine nei confronti di Apple stessa.

In base all'analisi della Commissione, le condizioni commerciali applicate da Apple agli sviluppatori di *App* violano l'art. 5, par. 4, in quanto limitano in modo ingiustificato la loro capacità di indirizzare i

[101] V. Booking Holdings Inc.'s Digital Markets Act Compliance Report - Public Summary November 2025, secondo cui: «Booking.com complies with Art. 5(3) DMA by ensuring that its partners are not subject to parity requirements for inventory in the EEA, or conditions to participate on Booking.com's platform that effectively prevent them from offering better prices or conditions for inventory in the EEA on other channels.»

[102] Commissione europea, decisione del 4 marzo 2024, Caso AT.40437 – *Apple – App Store Practices (music streaming)*.

propri utenti verso offerte esterne, imponendo vincoli tecnici, obblighi informativi e oneri economici per le transazioni concluse al di fuori dell'*App Store*. La Commissione ha, quindi, sanzionato la società al pagamento di un'ammenda pari a 500 milioni di euro.

Per quanto riguarda, invece, gli obblighi che necessitano di specificazioni ulteriori, l'art. 6, par. 5, DMA introduce il divieto di *self-preferencing*[103]. Si tratta di una fattispecie che ricalca fedelmente le decisioni della Commissione europea in materia di abuso di posizione dominante *ex* art. 102 TFUE assunte, in tale contesto, nei confronti sia di *Google* (ad oggi *Alphabet*)[104] che di Amazon[105]. A testimonianza di ciò, il divieto in esame è stato tra i primi a essere sottoposto all'esame della Commissione, la quale ha aperto un'indagine formale, *ex* art. 29 DMA, nei confronti di *Alphabet Inc*., quale fornitore del motore di ricerca generalista *Google Search*[106]. Nonostante le misure adottate da Alphabet per il rispetto dell'art. 6, par. 5, DMA[107], la Commissione ha rilevato che servizi verticali *Google Flights*, *Google Maps*, *Google Hotels* beneficiano di un posizionamento privilegiato nei risultati ("*Search Engine Results Page*" o cd. "SERP") dell'omonimo motore di ricerca, ottenendo maggiore visibilità e integrazione rispetto ai servizi concorrenti. Analoghe preoccupazioni sono state sollevate con riguardo a *YouTube*, rispetto al quale i contenuti generati o sponsorizzati da *Alphabet* hanno beneficiato di un trattamento preferenziale nei sistemi di ricerca e raccomandazione, a discapito di contenuti analoghi pubblicati sulla piattaforma da operatori terzi.

5. Conclusioni

Dall'analisi condotta possono trarsi alcune considerazioni conclusive.

[103] M. PEITZ, *The Prohibition of Self-preferencing in the DMA* – CERRE Report, 2022; I. GRAEF, *Differentiated Treatment in Platform-to-Business Relations: EU Competition Law and Economic Dependence*', in *Yearbook of European Law*, 2019, p. 448.

[104] Commissione europea, decisione *Google Search (Shopping)*, cit.; Commissione europea, decisione del 18 luglio 2018, Caso AT.40099, *Google Android*.

[105] Commissione europea, decisione del 10 novembre 2020, Caso AT.40462, *Amazon Marketplace*.

[106] Commissione europea, decisione del 25 marzo 2024, DMA.100193, *Alphabet - Online Search Engine - Google Search* - Art. 6(5).

[107] Cfr. Alphabet, EU Digital Markets Act (EU DMA) Compliance Report - Non-Confidential Summary, del 7 marzo 2025, p. 200 in cui si precisa che: «Google Shopping already complied with Art. 6(5) prior to the DMA. It ranks and displays results for offers in the same way irrespective of whether they are provided by Google or third parties. Google Shopping did so prior to the DMA's adoption.»

Il DMA, pur presentandosi formalmente come strumento regolatorio dei mercati digitali e qualificando espressamente la sua applicazione "senza pregiudizio" nei confronti degli artt. 101 e 102 TFUE e delle corrispondenti norme nazionali, rappresenta una forma inedita di intervento pubblico.

Da un lato, la sua adozione aderisce ai tre criteri stabiliti dalla Commissione europea nel mercato delle comunicazioni elettroniche e impone – temporaneamente ed *ex ante* – obblighi dettagliati e non contestabili tramite giustificazioni economiche a specifici settori, al fine di risolvere fallimenti di mercato diversi dal potere di mercato; esso può, pertanto, farsi rientrare nella categoria della regolamentazione economica.

Dall'altro lato, gli obblighi previsti dal DMA codificano la prassi applicativa dell'art. 102 TFUE al fine di raggiungere un obiettivo che è, piuttosto che complementare, assimilabile agli scopi prefissati dal diritto della concorrenza, e del cui rispetto si fa carico un'architettura istituzionale che trova proprio in quest'ultimo il suo referente teorico[108].

[108] Tanto le competenze attribuite dal DMA alla Commissione europea, quanto il suo quadro sanzionatorio rispecchiano l'architettura del regolamento (CE) n. 1/2003 in materia di applicazione degli artt. 101 e 102 TFUE. Sotto il profilo istruttorio, il DMA attribuisce alla Commissione la facoltà di condurre indagini di mercato (art. 17), richiedere informazioni ai *gatekeeper* e alle imprese interessate (art. 21), procedere ad audizioni e raccolta di dichiarazioni (art. 22) e svolgere ispezioni nei locali aziendali (art. 23). Inoltre, il DMA conferisce alla Commissione il potere di adottare nei confronti dei *gatekeeper* una «decisione relativa all'inosservanza» degli obblighi da esso stabiliti (art. 29), e atti di esecuzione per l'accettazione di impegni (art. 25) o per l'applicazione di misure provvisorie (art. 24) nel contesto di procedimenti già aperti ai sensi dell'art. 29, par. 1. Si tratta di un *corpus* di competenze mutuato, rispettivamente, dai capi V "Poteri di indagine" e III "Decisioni della Commissione" del regolamento 1/2003. Sul piano sanzionatorio, l'art. 30, par. 1, DMA, riprendendo la logica dell'art. 23, par. 2, reg. 1/2003, stabilisce che, nell'ambito della citata decisione relativa all'inosservanza *ex* art. 29 DMA, la Commissione possa irrogare ammende fino al 10% del fatturato mondiale realizzato dal *gatekeeper* nell'esercizio precedente, soglia che può raggiungere il 20% in caso di reiterazione della medesima o analoga violazione nell'arco degli otto anni precedenti. In aggiunta, l'art. 30, par. 3, DMA prevede sanzioni per le violazioni procedurali – sul modello dell'art. 23, par. 1, lett. a) - e), reg. 1/2003 – applicate dalla Commissione nella misura fino all'1% del fatturato mondiale qualora il *gatekeeper* ometta, ad esempio, di notificare il superamento delle soglie quantitative ai fini della designazione *ex* art. 3, par. 3, oppure non adempia agli obblighi informativi *ex* art. 14. Infine, l'art. 31 DMA introduce un regime di penalità di mora che, come già previsto dall'art. 24 reg. 1/2003, attribuisce alla Commissione il potere di imporre pagamenti periodici fino al 5% del fatturato medio giornaliero per ogni giorno di ritardo nell'osservanza degli obblighi da esso imposti. Sul tema dei poteri della Commissione europea nell'ambito del settore digitale v. O. PALLOTTA, *L'evoluzione "politica" dei poteri di vigilanza tecnica della Commissione europea*, in *questa Rivista*, 4/2025, p. 192.

Tale qualificazione ibrida del DMA non è priva di implicazioni problematiche sul piano applicativo, con riferimento alle aree di sovrapposizione individuate.

Innanzitutto, permangono dubbi relativi al potenziale cumulo degli interventi sanzionatori del DMA e del diritto della concorrenza e alla conseguente compromissione del principio del *ne bis in idem* sancito dall'art. 50 della Carta dei diritti fondamentali, pure espressamente richiamato dal considerando 109 DMA[109]. La sostanziale convergenza degli obiettivi del DMA rispetto a quelli perseguiti dal diritto antitrust, pare obliterarne la distintività sul piano formale, rischiando di esporre la medesima condotta di un *gatekeeper* a procedimenti paralleli condotti in applicazione delle due discipline[110].

Si tratta, a ben vedere, di tensioni che non riguardano esclusivamente l'ordinamento dell'Unione, potendosi estendere anche al piano nazionale. Come osservato, il DMA vieta agli Stati membri di introdurre obblighi aggiuntivi rivolti ai soli *gatekeeper*, al fine di perseguire gli obiettivi di equità e contendibilità dei mercati digitali. Tuttavia, i margini di operatività lasciati agli Stati membri potrebbero essere forieri dell'applicazione parallela del DMA e di normative nazionali adottate *ex* art. 1, par. 6, con l'effetto di estendere il rischio di cumulo sanzionatorio su entrambi i piani, nazionale e dell'UE.

A ciò si aggiunge la *governance* decentralizzata *ex* art. 38, par. 7 che attribuisce alle autorità nazionali competenti delle suddette normative nazionali il potere di indagine sul rispetto degli obblighi del DMA, con potenziali applicazioni disomogenee e contrastanti tra i vari Stati membri.

Un secondo ordine di problematiche attiene all'impianto degli obblighi del DMA, proiettato verso una logica di superamento della disciplina antitrust ("*enforcement failure*")[111]. In tal senso, la trasposizione, in forma *ex ante* e immediatamente applicabile, di rimedi già sperimentati nella recente prassi antitrust sembra riflettere la volontà di superare la complessità delle relative indagini e l'inefficacia dei rimedi *ex post*, piuttosto che fondarsi su una diagnosi dei fallimenti di mercato di

---

[109] A. GIANNACCARI, *Corte di giustizia Ue, tutela della concorrenza e principio del «*ne bis in idem*»*, in *Mercato Concorrenza Regole*, 1/2019, p. 157.

[110] A. ENGEL, X. GROUSSOT, E. HOLMBERG, *The Digital Markets Act and the Principle of Ne Bis in Idem: A Revolution in the Enforcement of EU Competition Law?*, in A. ENGEL, X. GROUSSOT, G.T. PETURSSON, (a cura di) *New Directions in Digitalisation. European Union and its Neighbours in a Globalized World*, 2024, Cham, p. 187.

[111] G. COLANGELO, *DMA, begins*, cit., p. 8; M. CAPPAI, G. COLANGELO, *Taming digital gatekeepers: the 'more regulatory' approach to antitrust law*, p. 5.

ciascun SPB, anche a causa dell'appiattimento di quest'ultimo concetto ad un coacervo eterogeneo di caratteristiche senza alcuna pretesa definitoria.

Un approccio che potrebbe anche minare il principio di proporzionalità a fondamento del regolamento[112]. Mentre alcune previsioni – quali l'obbligo *anti-steering*, il divieto di limitare il *multi-homing*, o le imposizioni in materia di trasparenza verso inserzionisti e editori previsti, rispettivamente, dagli artt. 5, par. 4, 6, par. 6, e 5, parr. 9 e 10 – si riferiscano a pratiche considerabili *prima facie* sleali, altri, invece, – quali i divieti indirizzati alle clausole MFN e alle tecniche di *self-preferencing* di cui agli art. 5, par. 3, e 6, par. 5 – si rifanno a fattispecie identificate dalla prassi antitrust come ambigue, sotto il profilo del bilanciamento degli effetti anti e pro-competitivi.

L'assenza di un'analisi caso per caso per l'implementazione di questi obblighi rischia di condurre ad esiti sproporzionati rispetto agli obiettivi di equità e contendibilità prefissati dal DMA. Questa problematica, inoltre, risulta solo parzialmente mitigata dai meccanismi di specificazione previsti dall'art. 8 con riferimento agli obblighi di cui all'art. 6 – in quanto, come osservato, tale procedimento è a totale discrezione della Commissione europea – e risulta, di contro, amplificata dai ristretti margini operativi delle eccezioni opponibili dai *gatekeeper*, *ex* art. 3, par. 5, alla loro soggezione a dette norme[113].

Infine, in chiave più ampia, occorre interrogarsi sul rischio che il DMA costituisca un freno non solo all'innovazione, come lamentato da alcuni *gatekeeper*[114] e da consessi ufficiali Statunitensi[115], ma all'intera strategia digitale europea. Il DMA si inserisce nella folta schiera di atti fondati sull'art. 114 TFUE al fine di realizzare il Mercato Unico Digitale. In questa prospettiva esso non costituisce un intervento regolatorio isolato, ma si inserisce in un quadro normativo stratificato che comprende, tra gli altri, il Regolamento (UE) 679/2016 ("GDPR"), il Regolamento (UE) 2019/1150 sulle relazioni tra piattaforme e utenti commerciali ("P2B"), il

---

[112] A. LAMADRID DE PABLO, N. BAYÓN FERNÁNDEZ, *Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and How to Fix It*, cit., p. 580 ss.

[113] Monopolkommission, Recommendations for an effective and efficient Digital Markets Act - Special Report 82 by the Monopolies Commission pursuant to section 44 subsection (1), sentence 4, of the German Act against Restraints of Competition, 2021, p. 43.

[114] V. Apple Statement, *The Digital Markets Act's impacts on EU users*, 24 settembre 2025, disponibile online all'indirizzo https://www.apple.com/newsroom/2025/09/the-digital-markets-acts-impacts-on-eu-users/.

[115] U.S. House of Representatives, Committee on the Judiciary, Hearing on Competition in Digital Markets, 2021.

Regolamento (UE) 2022/2065 ("Digital Services Act"), il Regolamento (UE) 2023/2854 ("Data Act") e il Regolamento (UE) 2022/868 ("Data Governance Act"), con i quali forma un sistema integrato di disciplina dell'economia digitale[116]. Da un lato, queste normative riflettono la strategia dell'Unione di creare standard normativi in grado di influenzare, a livello globale, il comportamento degli operatori, secondo la logica del cd. *Brussels effect*[117]. Dall'altro lato, il loro stretto rapporto, in uno con lo scarso coordinamento reciproco, rischia di estendere le problematiche che affliggono un singolo atto all'intero impianto normativo digitale, come rappresentato dalla recente proposta *Digital Omnibus* della Commissione europea[118], sottoposta a rilievi critici in merito alla riduzione del livello della protezione dei dati consolidato dal GDPR, attuando una sorta di "*anti-Brussels effect*"[119].

Il DMA va, dunque, inteso quale intervento ibrido, che si colloca al crocevia tra regolazione e politica della concorrenza e la cui efficacia dipenderà dalla capacità della Commissione e delle autorità nazionali sia di garantire un'applicazione coerente, evitando sovrapposizioni ingiustificate con il diritto antitrust dell'UE e, soprattutto, nazionale, sia di preservare, oltre l'equità e la contestabilità, uno spazio adeguato all'innovazione, la crescita e la competitività del Mercato Unico Digitale[120], facendo leva sui suoi margini di adeguamento al progresso tecnologico e sulla transitorietà del suo impianto normativo.

---

[116] Sull'interazione del DMA con altri atti adottati dall'UE nel settore digitale v. G. MONTI, A. DE STREEL, *Interplay Between the DMA and Other Regulations - Issue Paper DMA Implementation Forum*, CERRE Issue Paper - DMA Implementation Forum, 2025.

[117] A. BRADFORD, The Brussels Effect. How the European Union Rules the World, Oxford, 2020.

[118] Commissione europea, Proposal for a Regulation 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), COM(2025) 837 def.

[119] M. CALAMARI, Digital Omnibus, la resa dell'Unione Europea sui diritti digitali?, Agenda Digitale del 25 novembre 2025, disponibile online all'indirizzo https://www.agendadigitale.eu/sicurezza/privacy/digital-omnibus-la-resa-dellunione-europea-sui-diritti-digitali/; J. THORNHILL, Europe's tech sector is evolving fast. Is it fast enough?, Financial Times del 20 novembre 2025, disponibile online all'indirizzo https://www.ft.com/content/6e8706c8-6227-489d-9e1b-d5205697d4e7.

[120] Interpretazione, questa, confermata dalla Commissaria M. Vestager nel proprio discorso "Competition policy: where we stand and where we're going", tenutosi a Bruges il 25 marzo 2022. V. F. SPORTA CAPUTI, Il Digital Market Act (Reg.to UE n. 2022/1925) ed il nuovo approccio alla regolazione ex ante dell'abuso di posizione dominante, cit., p. 71; G. COLANGELO, DMA, Begins, cit., p. 9.